

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

1c893 U.S. PTO
09/653416
08/31/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

出 願 年 月 日
Date of Application:

1999年 9月28日

出 願 番 号
Application Number:

平成11年特許願第274182号

出 願 人
Applicant(s):

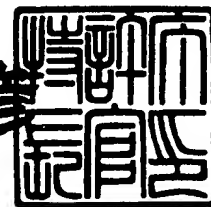
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 6月23日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3046787

【書類名】 特許願
【整理番号】 2032710022
【提出日】 平成11年 9月28日
【あて先】 特許庁長官殿
【国際特許分類】 G11B 19/02
G11B 27/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 廣田 照人

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 田川 健二

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【プルーフの要否】 不要

【書類名】 明細書

【発明の名称】 情報処理装置と課金処理装置

【特許請求の範囲】

【請求項 1】 記録メディアにデジタルデータを記録する情報処理装置であって、

ユーザから少なくともデジタルデータの取得要求を受け付ける入力読取り手段と、

外部から超流通形式のデジタルデータを受信する超流通形式データ受信手段と、

超流通形式のデジタルデータを記録する超流通形式データ記憶領域と、

前記超流通形式データ記憶領域から超流通形式のデジタルデータを取出すデータ取出し手段と、

超流通形式のデジタルデータに記録された課金情報に従って、外部の課金サーバと交信し、購入処理を行って、コンテンツを復号化する鍵を取出す購入処理手段と、

購入処理手段によって取出された、コンテンツを復号化する鍵、個人を特定できるユーザ ID、権利情報を記録するセキュアデータ記憶領域と、

前記セキュアデータ記憶領域から個人を特定できる ID を取出し、配布元ユーザ ID として、前記データ取出し手段によって取出された超流通形式のデジタルデータに、追加する配布元ユーザ ID 付加手段と、

前記配布元ユーザ ID 付加手段によって、新たに配布元ユーザ ID を付加された超流通形式のデジタルデータを記録メディアに記録するコンテンツ記録手段を備えることを特徴とする情報処理装置。

【請求項 2】 記録メディアにデジタルデータを記録する情報処理装置であって、

前記超流通形式のデジタルデータから取出したコンテンツを復号化する鍵を用いてコンテンツを復号化し、記録メディアが持つ固有の ID を取得して、これを鍵とし、コンテンツを再暗号化し、超流通形式のコンテンツの再生制御情報を元に、記録メディア固有の ID を用いて暗号化したコンテンツの再生制御情報を生成

して、データ形式を変換するデータ形式変換手段を備えることを特徴とする請求項 1 記載の情報処理装置。

【請求項 3】 記録メディアに記録されたデジタルデータを再生する情報処理装置であって、

前記セキュアデータ記憶領域から暗号化コンテンツを復号化するための鍵を取出し、これを利用して前記データ取出し手段によって取出された超流通形式データから、暗号化コンテンツを復号化するコンテンツ復号手段と、

前記コンテンツ復号手段によって復号化されたコンテンツを再生する再生手段を備えたことを特徴とする、請求項 2 記載の情報処理装置。

【請求項 4】 デジタルデータを記録メディアに記録する情報処理装置であって、

前記データ取出し手段によって取出された超流通形式データに含まれる課金情報を取出す課金情報取出し手段と、

前記課金情報取出し手段によって取出された課金情報を、課金処理を行う課金サーバへ送信する課金情報送信手段と、

前記データ取出し手段によって取出された超流通形式のデータに配信元ユーザ ID が付加されているかどうかを判定し、付加されている場合には、課金情報に配信元ユーザ特定情報も付加して送信するよう課金情報送信手段に指示する配信元ユーザ特定情報有無判定手段を有することを特徴とする請求項 3 記載の情報処理装置。

【請求項 5】 課金情報に基づいて、課金処理を行う課金処理装置であって、前記課金情報送信手段によって送信された課金情報を受信する課金情報受信手段と、

前記送信元ユーザ ID 送信手段によって送信されたユーザ ID を受信して、送信元ユーザを特定する送信元ユーザ特定手段と、

前記課金情報受信手段によって受信された課金情報に従って、前記送信元ユーザ特定手段によって特定されたユーザに対して課金処理を行う課金処理手段と、

前記課金情報受信部で受信したデータに、前記配信元ユーザ ID が付加されている場合、配布元ユーザ ID 取出す、配布元ユーザ ID 取出し手段と、

前記暗号化された配信元ユーザ I D を復号化する配信元ユーザ I D 復号手段と

配布元ユーザ I D により指定されたユーザに対し特典を与える特典処理を行う特典処理手段とを備えることを特徴とする課金処理装置。

【請求項 6】 記録メディアから超流通形式データのコンテンツを再生する情報処理装置であって、

記録メディアに記録されているコンテンツから、少なくともユーザからの再生するコンテンツを選択入力を受け取る入力読取り手段と、

前記入力読取り手段によって暗号化されたコンテンツが、他のメディアへの移動が許された超流通形式のコンテンツか、許されていないコンテンツかを判別するデータ判別手段と、

記録メディアから再生に必要なデータと暗号化されたコンテンツと、前記データ判別手段の結果が、メディア固有の I D を用いて暗号化されたコンテンツであれば、記録メディアから固有の I D を鍵として読取り、超流通形式のデータであれば、コンテンツを復号化する鍵を読取るデータ読取り手段と、

読取り手段から暗号化されたコンテンツと、暗号化されたコンテンツを復号化する鍵を受け取り、復号化する復号手段と、

再生に必要なデータを読み取り、データの位置と時間情報をリンクさせた再生を制御するデータを解釈する再生制御手段と、

復号化されたコンテンツをデコードし、外部出力手段に音声出力を指示する再生手段を備えることを特徴とする情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンテンツ著作権保護方式に関し、より特定的には、超流通形式のデータと超流通形式でないデータが記録された記録メディア、および前記記録メディアへデータを記録し、超流通形式のデータを再生する情報処理装置と、超流通形式のデータに対し課金処理を行う課金処理装置に関する。

【0002】

【従来の技術】

近年、インターネット上におけるコンテンツの有料配布、いわゆるEC (Electronic Commerce: 電子商取引) が普及し始めており、多くの有料コンテンツが提供されている。インターネットによるECでは、一般的に情報提供者が開設したホームページに消費者がアクセスし、好みのコンテンツを検索する。好みのコンテンツがあった場合、消費者はコンテンツの購入要求に加え、ユーザIDやクレジットカードの番号などを情報提供者に通知することによって課金処理を行う。そして、コンテンツを直接ダウンロードすることが可能となる。

【0003】

また、ECの対象となるデジタルデータは、その情報の劣化がほとんど生じないために極めて品質が高いという特徴を有する。そして、圧縮技術の進歩によって、音楽や映像といったデータ（コンテンツ）のECを通じた配信が可能となってきている。

【0004】

しかしこういった技術の進展により問題が起きた。MP3 (MPEG1 Audio Layer3) がそれである。MP3は音声データの圧縮技術で、CDの音楽データをほとんど音質を劣化させることなく、約10分の1に圧縮することができる。MP3のPC用エンコーダおよびデコーダはインターネットでユーザが無償で手に入れることができる。ユーザはエンコーダを用いてCDの音楽データをエンコードしてMP3のデータを作成し、ネットワークを通じてその音楽データを再配布することが可能となり、このような利用形態に対しては音楽データの著作権保護が難しくなってきた。

【0005】

こういった事態を重く見た音楽業界は、ネットワークを通じた音楽配信においても著作権保護の守られる仕組みを規定するための団体・SDMI (Secure Digital Music Initiative) を発足させた。このSDMIの規定では、インターネットなどを通じて得た電子音楽コンテンツは、一旦記録メディアに記録されると、著作権保護が保証されない限り、他のメディアへコンテンツを移動することは許していない。

【 0 0 0 6 】

これを実現するために記録メディアには固有の I D を付与し、これに記録される電子音楽コンテンツは固有の I D を利用して暗号化する仕組みを採択した。仮にこの暗号化されたデータを他のメディアに移動、もしくはコピーしたとしても、暗号化に用いられた I D と記録メディアの I D が一致しないために再生することができない。よって、著作権保護が保証される。

【 0 0 0 7 】

また、超流通を実現するために、コンテンツを暗号化し、その鍵とコンテンツ購入の課金情報をさらにまとめて暗号化し、超流通形式のデータとして、データがコピーされても課金が行われる仕組みが考えられている。

【 0 0 0 8 】

すなわち、インターネット等で音楽コンテンツを記録メディアにダウンロードする際には課金が行われ、記録メディアに記録された音楽コンテンツは他メディアへの複写をさせないことにより音楽コンテンツの著作権の保護を図ろうとしている。

【 0 0 0 9 】

【発明が解決しようとする課題】

しかしながら、前述のような記録メディアの固有の I D を用いてコンテンツを暗号化、記録メディアに記録するのでは、音楽コンテンツが記録メディアにダウンロードされた時点で課金処理が可能な超流通が終了することになり、ダウンロードしたユーザが二次配信元となり超流通を継続させることができない。

【 0 0 1 0 】

すなわち、ダウンロードユーザが、ダウンロードしたデジタルデータを記録メディアに記録した場合、記録メディアをさらに二次配信元として配布でき、かつ、著作権保護者が複写配布された記録メディアに対して課金処理を行うことができない問題点があった。

【 0 0 1 1 】

そこで本発明は、このような従来の問題点に則して考えられたものであって、より具体的には、超流通によりデジタルデータをダウンロードし、それを記録

メディアに記録するとき、二次配信が可能なデータ形式で記録メディアに記録し、かつ、二次配信されたデジタルデータに対しても著作権保護者が課金処理を行える情報処理装置と課金処理装置を提供することを目的とする。

【0012】

また、記録メディアから超流通形式のデジタルデータをアップロードして、記憶領域に記録、もしくは記録メディアの固有のIDを用いて暗号化されたコンテンツを超流通形式のデジタルデータに変換するための情報とともにアップロードして、それぞれ適切な記憶領域に記録し、そのデータを管理する情報処理装置を提供することを目的とする。

【0013】

さらに、前記記録メディアを得た第三者がその二次配信された超流通形式のデジタルデータを購入した場合、二次配信の配信元となったユーザや記録に使われたソフトウェアベンダー、前記記録メディアのベンダーが、何らかのメリットを享受できる情報処理装置を提供することを目的とする。

【0014】

また、超流通形式の音楽データの記録を実現する記録メディアの提供を目的とする。また、超流通形式の音楽データを記録した、前記記録メディアからデジタルデータを読み取り、コンテンツを再生することのできる情報処理装置を提供することを目的とする。

【0015】

【課題を解決するための手段】

この課題を解決するために、本発明の情報処理装置は、ユーザから少なくともデジタルデータの取得要求を受け付ける入力読取り手段と、外部から超流通形式のデジタルデータを受信する超流通形式データ受信手段と、超流通形式のデジタルデータを記録する超流通形式データ記憶領域と、前記超流通形式データ記憶領域から超流通形式のデジタルデータを取出すデータ取出し手段と、超流通形式のデジタルデータに記録された課金情報に従って、外部の課金サーバと交信し、購入処理を行って、コンテンツを復号化する鍵を取出す購入処理手段と、購入処理手段によって取出された、コンテンツを復号化する鍵、個人を特定で

きるユーザID、権利情報を記録するセキュアデータ記憶領域と、前記セキュアデータ記憶領域から個人を特定できるIDを取出し、配布元ユーザIDとして、前記データ取出し手段によって取出された超流通形式のデジタルデータに、追加する配布元ユーザID付加手段と、前記配布元ユーザID付加手段によって、新たに配布元ユーザIDを付加された超流通形式のデジタルデータを記録メディアに記録するコンテンツ記録手段を備えることを特徴としている。

【0016】

また、本発明の情報処理装置は、前記超流通形式のデジタルデータから取出したコンテンツを復号化する鍵を用いてコンテンツを復号化し、記録メディアが持つ固有のIDを取得して、これを鍵とし、コンテンツをもう一度暗号化し、超流通形式のコンテンツの再生制御情報から、記録メディア固有のIDを用いて暗号化したコンテンツの再生制御情報を生成して、データ形式を変換するデータ形式変換手段を備えることを特徴としている。

【0017】

また、本発明の情報処理装置は、前記セキュアデータ記憶領域から暗号化コンテンツを復号化するための鍵を取出し、これを利用して前記データ取出し手段によって取出された超流通形式データから、暗号化コンテンツを復号化するコンテンツ復号手段と、前記コンテンツ復号手段によって復号化されたコンテンツを再生する再生手段を備えたことを特徴としている。

【0018】

また、本発明の情報処理装置は、前記データ取出し手段によって取出された超流通形式データに含まれる課金情報を取出す課金情報取出し手段と、前記課金情報取出し手段によって取出された課金情報を、課金処理を行う課金サーバへ送信する課金情報送信手段と、前記データ取出し手段によって取出された超流通形式のデータに配信元ユーザIDが付加されているかどうかを判定し、付加されている場合には、課金情報に配信元ユーザ特定情報も付加して送信するよう課金情報送信手段に指示する配信元ユーザ特定情報有無判定手段を有することを特徴としている。

【0019】

また、本発明の課金処理装置は、前記課金情報送信手段によって送信された課金情報を受信する課金情報受信手段と、前記送信元ユーザ I D 送信手段によって送信されたユーザ I D を受信して、送信元ユーザを特定する送信元ユーザ特定手段と、前記課金情報受信手段によって受信された課金情報に従って、前記送信元ユーザ特定手段によって特定されたユーザに対して課金処理を行う課金処理手段と、前記課金情報受信部で受信したデータに、前記配信元ユーザ I D が付加されている場合、配布元ユーザ I D 取出す、配布元ユーザ I D 取出し手段と、前記暗号化された配信元ユーザ I D を復号化する配信元ユーザ I D 復号手段と、配布元ユーザ I D により指定されたユーザに対し特典を与える特典処理を行う特典処理手段とを備えることを特徴としている。

【 0 0 2 0 】

また、本発明の情報処理装置は、記録メディアに記録されているコンテンツから、少なくともユーザからの再生するコンテンツを選択入力を受け取る入力読取り手段と、前記入力読取り手段によって暗号化されたコンテンツが、他のメディアへの移動が許された超流通形式のコンテンツか、許されていないコンテンツかを判別するデータ判別手段と、記録メディアから再生に必要なデータと暗号化されたコンテンツと、前記データ判別手段の結果が、メディア固有の I D を用いて暗号化されたコンテンツであれば、記録メディアから固有の I D を鍵として読取り、超流通形式のデータであれば、コンテンツを復号化する鍵を読取るデータ読取り手段と、読取り手段から暗号化されたコンテンツと、暗号化されたコンテンツを復号化する鍵を受け取り、復号化する復号手段と、再生に必要なデータを読み取り、コンテンツの C o d e c や、データの位置と時間情報をリンクさせるなどの再生を制御するデータを解釈する再生制御手段と、復号化されたコンテンツをデコードし、外部出力手段に音声出力を指示する再生手段を備えることを特徴としている。

【 0 0 2 1 】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら説明する。

【 0 0 2 2 】

(実施の形態 1)

図 1 は、本発明における情報処理装置であるデジタルデータ記録再生装置 101 (a) ~ 101 (c)、コンテンツサーバ 102、課金サーバ 103、記録メディア 104、デジタルデータ再生装置 105 の関係を表わした図である。

【0023】

デジタルデータ記録再生装置 101 (a) ~ 101 (c)、コンテンツサーバ 102、課金サーバ 103 間の通信はインターネットなどの通信手段を用いて行われる。デジタルデータ記録再生装置 101 (a) ~ 101 (c) は一般的にはパーソナルコンピュータで実現され、受け取るデジタルデータはインターネットなどを通じて配信される、もしくは半導体メディアなどの記録メディアに記録されているものとする。

【0024】

なお、通信手段はインターネットでなく、衛星放送、CATVなどで行われてもよい。またデジタルデータ記録再生装置 101 (a) ~ 101 (c) はSTB (Set Top Box) などで実現されてもよい。

【0025】

また、本実施の形態で扱われるコンテンツは、以後電子音楽データ (AAC (Advanced Audio Coding)、LPCM (Linear Pulse Code Modulation)、DTS (Digital Theater system)、MP3 (MPEG1 Audio Layer3) などのデータを電子音楽データと称す) であるとするが、これに限られたものではなく、電子新聞、電子マガジン、電子BOOK、電子マップ、電子辞書、ビデオ、静止画、ゲーム、コンピュータ用ソフトウェアツール、などのデジタルコンテンツでもよい。

【0026】

まず本実施の形態で使用するデータのデータ構造の説明を行う。

【0027】

図 2 は、本発明においてコンテンツが配信されるときデータのデータ構造であり、記録メディアに記録されたときも、他のメディアへの移動の許された、超流通形式のデータ構造である。超流通形式のデータ構造は、コンテンツを暗号化する鍵 201、課金情報 202、データ 203、コンテンツ 204 で構成される。また鍵

2 0 1、課金情報 2 0 2 は結合された形でまとめて暗号化されており、暗号化ヘッダ部 2 1 0 と称する。この暗号化は例えば、R S A 暗号方式のように、公開鍵方式で行われる。すなわち、暗号化したキーと、復号化するためのキーが異なることを示す。またコンテンツ 2 0 4 は鍵 2 0 1 を使って暗号化されており、これを暗号化コンテンツ部 2 2 0 と称する。この暗号化は例えば、秘密鍵暗号方式で行われる。さらに暗号化ヘッダ部 2 1 0、データ 2 0 3、暗号化コンテンツ部 2 2 0 は結合されており、これを第一の超流通形式データ 2 3 0 と称する。以後、各構成要素について説明する。

【 0 0 2 8 】

鍵 2 0 1 は後述するコンテンツ 2 0 4 を復号化するための鍵である。課金情報 2 0 2 にはコンテンツを再生、購入するときの課金額などが記述される。データ 2 0 3 には暗号化を必要としないデータが記録される。コンテンツ 2 0 4 は例えば電子音楽データであり、鍵 2 0 1 で暗号化されている。

【 0 0 2 9 】

以降、図 2 のようなデータ構造をとるデジタルデータを第一の超流通形式データ 2 3 0 と呼ぶ。

【 0 0 3 0 】

図 3 は、ユーザを特定できる、ユーザ I D を暗号化して暗号化 I D 部 3 1 0 とし、第一の超流通形式データ 2 3 0 に付加して、第二の超流通形式データ 3 2 0 としたものである。

【 0 0 3 1 】

以上で、本実施の形態で使用するデータのデータ構造の説明を終わる。

【 0 0 3 2 】

次に、本実施の形態で使用する記録メディア 1 0 4 の説明を行う。

【 0 0 3 3 】

図 4 は、本発明において扱われる記録メディア 1 0 4 のデータエリアの構成図である。記録メディア 1 0 4 はセキュアデータエリア 4 0 1、第一のエリア 4 0 2、第二のエリア 4 0 3 から構成される。以後、各構成要素について説明する。

【 0 0 3 4 】

セキュアデータエリア 4 0 1 には復号化の鍵、ユーザの個人情報、権利情報など、第 3 者からのアクセスが許されないデータが記録される。第一のエリア 4 0 2 には超流通形式のデータ構造をもつ図 2 および図 3 のデータが記録される。第二のエリア 4 0 3 には記録メディアの ID を用いて暗号化された移動することが許されないデータ形式を持つデータなどが記録される。

【 0 0 3 5 】

以上で、本実施の形態で使用する記録メディア 1 0 4 の説明を終わる。

【 0 0 3 6 】

次に、本実施の形態におけるデジタルデータ記録再生装置の説明を行う。

【 0 0 3 7 】

図 5 は、デジタルデータ記録再生装置 1 0 1 (a) の構成を示す図である。デジタルデータ記録再生装置 1 0 1 (a) は、一般にはパーソナルコンピュータで実現され、ユーザ入力読取り手段 5 0 0、超流通形式データ受信手段 5 0 1、超流通形式データ記憶領域 5 0 2、データ取出し手段 5 0 3、配布元ユーザ ID 付加手段 5 0 4、コンテンツ記録手段 5 0 5、購入処理手段 5 0 6、セキュアデータ記憶領域 5 0 7、コンテンツ復号手段 5 0 8、再生制御手段 5 0 9、再生手段 5 1 0、外部出力手段 5 1 1、第一のデータ形式変換手段 5 1 2、第二のデータ形式変換手段 5 1 3 から構成される。

【 0 0 3 8 】

ユーザ入力読取り手段 5 0 0 は、具体的にはキーボードやマウスによって実現され、超流通形式データ受信手段 5 0 1 によって、受信を希望するデジタルデータや、超流通形式データ記憶領域 5 0 2 にあるデジタルデータを再生したり、記録メディアに記録するといったユーザからの入力を読み取る。

【 0 0 3 9 】

超流通形式データ受信手段 5 0 1 は、ユーザ入力読取り手段 5 0 0 から読取ったユーザからの要求に基づいて、コンテンツサーバ 1 0 2 から、第一の超流通形式データ 2 3 0、もしくは第二の超流通形式データ 3 2 0 を受信し、超流通形式データ記憶領域 5 0 2 に記録する。

【 0 0 4 0 】

また、超流通形式データ受信手段501は、ユーザ入力読取り手段500から読取ったユーザからの要求に基づいて、要求したデジタルデータが超流通形式データであれば記録メディア104から受信し、そのままのデータ形式で超流通形式データ記憶領域502に記録する。このとき記録メディア104のセキュアデータエリア401に記録された、コンテンツの記録許可回数が記述された権利情報を取り出し、セキュアデータ記憶領域507に記録する。ユーザが要求したデジタルデータが記録メディア固有のIDを用いて暗号化されたデジタルデータの場合は、第二のデータ形式変換手段513でデータ形式を超流通形式データに変換し、超流通形式データ記憶領域502に記録する。このとき記録メディア104のセキュアデータエリア401に記録された、コンテンツの記録許可回数が記述された権利情報を取り出し、セキュアデータ記憶領域507に記録する。

【0041】

以上のような、デジタルデータ記録再生装置101(a)が記録メディア104から、デジタルデータを取得し、超流通形式データ記憶領域502に記録する動作を、図11を用いて説明する。

【0042】

デジタルデータ記録再生装置101(a)は、ユーザ入力読取り手段500によって受取ったユーザ要求に基づいて、超流通形式データ記憶領域502に記録するデジタルデータを記録メディア104から取り出し、デジタルデータが超流通形式のデータである場合は(S1101)、超流通形式データを復号化する鍵と、記録されたデータの記録許可回数が記述された権利情報を記録メディア104のセキュアデータエリア401から取り出し、セキュアデータ記憶領域507に記録する(S1102)。そして、超流通形式データ受信手段501は、超流通形式データを記録メディア104から取り出し、超流通形式データ記憶領域502に記録する(S1103)。

【0043】

取り出すデジタルデータが超流通形式でない、記録メディア104の固有IDを用いて暗号化されたデジタルデータの場合(S1101)、記録メディア104のセキュアデータエリア401に記録された暗号化ヘッダ部210をセキュア

データ記憶領域 5 0 7 に記録する (S 1 1 0 4)。第二のデータ形式変換手段 5 1 3 にて、記録メディア 1 0 4 から固有 ID を取得して、前述のデジタルデータを復号化し、暗号化ヘッダ部 2 1 0 にある鍵 2 0 1 を利用して、復号化したコンテンツを暗号化する。また、この暗号化したコンテンツの再生制御情報を、前述の超流通形式でないデジタルデータの再生制御情報から生成する。この再生制御情報、暗号化したデジタルデータ、暗号化ヘッダ部 2 1 0 から超流通形式のデータを生成し (S 1 1 0 5)、超流通形式データ記録領域 5 0 2 に記録する (S 1 1 0 3)。

【 0 0 4 4 】

なお、再生制御情報には、再生すべきコンテンツの記録されている位置情報、コンテンツの圧縮形式、コンテンツを再生したときの再生経過時間とコンテンツの位置の対応情報が記述されている。また、超流通形式のデジタルデータと、記録メディア固有 ID を用いて暗号化されたデジタルデータの再生制御情報は形式が異なっている。

【 0 0 4 5 】

データ取出し手段 5 0 3 は、ユーザ入力読取り手段 5 0 0 から読取ったユーザからの要求に基づいて、超流通形式データ記憶領域 5 0 2 から超流通形式データを取り出す。

【 0 0 4 6 】

配布元ユーザ ID 付加手段 5 0 4 は、図 6 に示す通り、ユーザ ID 取得手段 6 0 1、ユーザ ID 暗号化手段 6 0 2、配布元ユーザ ID 結合手段 6 0 3 から構成される。ユーザ ID 取得手段 6 0 1 は、セキュアデータ記憶領域 5 0 7 にあるユーザ ID を取得し、ユーザ ID 暗号化手段 6 0 2 はユーザ ID 取得手段 6 0 1 によって取得されたユーザ ID を所定の暗号化方式で暗号化する。配布元ユーザ ID 結合手段 6 0 3 は、データ取出し手段 5 0 3 によって取出された第一の超流通形式のデータ 2 3 0 に、暗号化されたユーザ ID を付加し、第二の流通形式データ 3 2 0 を作成する。

【 0 0 4 7 】

以上のような、超流通形式データ記憶領域 5 0 2 に記憶された超流通形式のデ

ータに、ユーザIDを付加し、第二の超流通形式データ320を作成する動作について、図12に示すフローチャートを用いて説明する。

【0048】

ユーザID取得手段601は、セキュアデータ記憶領域507からユーザIDを取得し(S1201)、ユーザID暗号化手段602は取得されたユーザIDを所定の暗号化形式で暗号化する(S1202)。次に、データ取出し手段503は超流通形式データ記憶領域502から超流通形式データを取出し(S1203)、取出したデータが第二の超流通形式データ320かどうかを判定する(S1204)。第二の超流通形式データ320である場合は、第二の超流通形式データ320から第一の超流通形式データ230の部分を取出し(S1206)、暗号化されたユーザIDを付加して、第二の超流通形式のデータにする(S1206)。データが第二の超流通形式データ320でないと判定された場合は(S1204)、第一の超流通形式データ230を取出し(S1205)、暗号化されたユーザIDを付加して、第二の超流通形式のデータにする(S1206)。こうして作成された第二の超流通形式のデータを、記録メディア104の超流通形式データの記録される第一のエリア402へ、セキュアデータ記憶領域507に記録されてある、第二の超流通形式のデータの暗号化されたコンテンツを復号化する鍵と、このコンテンツの記録許可回数の記述された権利情報を記録メディア104のセキュアデータエリア401に記録する(S1207)。このとき、権利情報の他に二次配付されるときにその二次配付の元となった、ソフトウェアおよび二次配付の媒体となった記録メディアのベンダーを識別する情報をセキュアデータエリア401に記録することもできる。

【0049】

暗号方式変換手段512は、データ取出し手段503が超流通形式データ記憶領域502から取出した第一の超流通形式データ230、もしくは第二の超流通形式のデータ320の暗号化ヘッダ部210を復号化し、コンテンツを復号化する鍵201を取出し、コンテンツを復号化する。また、暗号方式変換手段512は記録メディア104から記録メディア固有のIDを取得し、これを暗号鍵として、前述の復号化されたコンテンツを暗号化し、暗号化ヘッダ部210とともにコ

コンテンツ記録手段505に送る。コンテンツ記録手段505は、暗号方式変換手段512から受取った暗号化されたコンテンツを記録メディア104の第二のエリア403に記録する。また、暗号化ヘッダ部210を記録メディア104のセキュアデータエリア401に記録する。このとき、権利情報の他に二次配付されるときにその二次配付の元となった、ソフトウェアおよび二次配付の媒体となった記録メディアのベンダーを識別する情報をセキュアデータエリア401に記録することもできる。

【0050】

購入処理手段506は、図7に示す通り、暗号化ヘッダ部取出し手段701、課金情報取出し手段702、配布元ユーザID取出し手段703、配布元ユーザID付加手段704、課金情報送信手段705、送信元ユーザID送信手段706、課金処理正常終了受信手段707、コンテンツ鍵取出し手段708、コンテンツ鍵書き込み手段709から構成される。暗号化ヘッダ部取出し手段701は、データ取出し手段503によって取出された超流通形式のデータから暗号化ヘッダ部210を取出す。課金情報取出し手段702は、暗号化ヘッダ部取出し手段701によって取出された暗号化ヘッダ部210から課金情報202を取出す。配布元ユーザID取出し手段703は、データ取出し手段503によって取出された超流通形式のデータにユーザIDが付加されているかどうか判定し、付加されている場合には、ユーザIDを取出し、配布元ユーザID付加手段704に対し、取出したユーザIDを付加するよう指示する。配布元ユーザID付加手段704は、課金情報取出し手段702によって取出された課金情報に、配布元ユーザID取出し手段703が取出したユーザIDを付加する。

【0051】

なお、ここでは受信した第二の超流通形式のデータの配布元ユーザIDを取出し、新たに配布元ユーザIDの上書きを行っているが、これは新たな配布元ユーザIDの追加でもよい。

【0052】

課金情報送信手段705は課金情報711を課金サーバ103に送信する。課金情報711は、図8に示す課金情報802にユーザID801を付加したデー

タ、もしくは課金情報のみからなるデータである。送信元ユーザID送信手段706は、課金情報送信手段705が課金情報711を送信すると同時に、セキュアデータ記憶領域507から取得したユーザIDを課金サーバへ送信する。課金処理正常終了受信手段707は、課金サーバ103から送信される課金処理が正常に終了したことを知らせる課金処理正常終了通知713を受信する。課金処理正常終了通知713が受信されると、コンテンツ鍵取出し手段708は暗号化ヘッダ部取出し手段701によって取出された暗号化ヘッダ部210からコンテンツ鍵を取出し、コンテンツ鍵書き込み手段709は取出されたコンテンツ鍵をセキュアデータ記憶領域507に書き込む。また課金処理正常終了通知713には、コンテンツの記録許可回数が記述された権利情報が含まれており、課金処理正常終了受信手段707は、この権利情報を権利情報書き込み手段714に送り、権利情報書き込み手段714は、受取った権利情報をセキュアデータ記憶領域507に記録する。

【0053】

セキュアデータ記憶領域507は、コンテンツ鍵と、ユーザIDおよび権利情報を記録しておく記憶領域であり、ユーザなどからはアクセスすることができないように保護されている記憶領域である。

【0054】

以上のような、超流通形式データ記憶領域502に記憶された超流通形式のデータを購入する際の動作について図13に示すフローチャートを用いて説明する。

【0055】

暗号化ヘッダ部取出し手段701は、データ取出し手段503によってとりだされた超流通形式データから暗号化ヘッダ部210を取出す(S1301)。取出された暗号化ヘッダ部210から、課金情報取出し手段702は、課金情報を取出す(S1302、S1303)。配布元ユーザID取出し手段703は、データ取出し手段503によって取出されたデータが第二の超流通形式データ320かどうかを判定し(S1304)、第二の超流通形式データ320の場合は、第二の超流通形式データ320からユーザIDを取出し(S1305)、取出し

たユーザIDを課金情報に付加する（S1306）。課金情報送信手段705は課金情報を課金サーバ103に送信し、送信元ユーザID送信手段706はセキュアデータ記憶領域507からユーザIDを取得し、取得したユーザIDを課金サーバ103に送信する（S1307）。

【0056】

上記の処理終了後、一定時間が経過した後、課金処理正常終了受信手段707は、課金サーバから課金処理正常終了通知713が送信されてきたかどうかを確認し、送信されてこない場合はS1307の処理に戻る（S1308）。課金処理正常終了通知が課金処理正常終了通知受信手段707に受信されると、コンテンツ鍵取出し手段708は、暗号化ヘッダ部210からコンテンツ鍵を取出し（S1309）、コンテンツ鍵書き込み手段709は取出したコンテンツ鍵をセキュアデータ記憶領域507に書き込む（S1310）。

【0057】

また課金処理正常終了通知713には、コンテンツの記録許可回数が記述された権利情報が含まれており、課金処理正常終了受信手段707は、この権利情報を権利情報書き込み手段714に送り、権利情報書き込み手段714は、受取った権利情報をセキュアデータ記憶領域507に記録する（S1311）。

【0058】

コンテンツ記録手段505は、配布元ユーザID付加手段504によって作成された第二の流通形式データ320を、記録メディア104の第一のエリア402に記録し、セキュアデータ記憶領域507に記録されている、前述の第二の流通形式データのコンテンツを解く鍵と、その権利情報を、記録メディアのセキュアデータエリアに記録する。

【0059】

権利情報にはコンテンツの記録許可回数、再生可能回数、購入情報が記述されており、セキュアデータ記憶領域507に記録されていた権利情報に、複数のコンテンツ記録許可回数、再生可能回数が記述されていた場合、これを分割することも可能である。

【0060】

なお、この権利情報は、本実施の形態ではセキュアデータエリア、および記録メディアに記録、管理することとしているが、権利情報管理の方法はこれによらず、サーバ側で管理する方法でもよい。

【0061】

再生制御手段509は、データ取出し手段503よりコンテンツの再生制御情報を受取る。また、コンテンツ復号手段508は、データ取出し手段503より暗号化されたコンテンツを受取り、それに対応した復号用の鍵をセキュアデータ記憶領域より受取り、この鍵を用いて前記暗号化されたコンテンツを復号化する。このとき記録メディア104に記録された権利情報が再生可能となっているかどうか確認するが、この権利情報がサーバなど、ネットワークで管理されている場合は、メールでその権利情報を送信するなどの方法でもよい。

【0062】

再生手段510は再生制御手段509に基づいて、コンテンツ復号手段508より受取った、復号化されたコンテンツをデコードし、外部出力手段511に音声データを出力するように指示する。

【0063】

以上のような、超流通形式データ記憶領域502に記憶された超流通形式データを再生する場合の動作について、図14に示すフローチャートを用いて説明する。

【0064】

コンテンツ復号手段508は、権利情報を参照し、再生しようとする超流通形式データが再生可能となっているかどうか確認する(S1401)。未購入である場合や再生のたびに課金処理を行う必要がある場合は、図13のフローチャートで示した購入プロセスを実行する(S1402)。コンテンツ復号手段508は、コンテンツ鍵を取得する(S1403)。コンテンツ復号手段508は、データ取出し手段503によって取出された超流通形式データから暗号化されたコンテンツを取出し(S1404)、S1403で取得した鍵を用いてコンテンツを復号化する(S1405)。復号化されたコンテンツは、再生制御手段509からの制御に基づいて、再生手段510でデコードされ、外部出力手段511に

よって音声が出力される（S1406）。

【0065】

また、ここでいう購入とは、必ずしも金銭のやりとりがあるものではなく、アンケートに答えたり、他のユーザを紹介するといった手段によっても実現されるコンテンツの利用を指す。広告の表示などにより、購入プロセスが実行されない場合もありうる。

【0066】

以上で、本実施の形態で使用するデジタルデータ記録再生装置101（a）の説明を終わる。

【0067】

次に、本実施の形態における課金サーバ103の課金処理装置901の説明を行う。

【0068】

図9は、課金サーバ103に備えられた課金処理装置901の構成を示す図である。課金処理装置901は、課金情報受信手段902、送信元認証手段903、課金処理手段904、課金処理正常終了通知手段905、配布元ユーザID取出し手段906、配布元ユーザID復号手段907、特典処理手段908によって構成される。課金情報受信手段902は購入処理手段506から送信された課金情報711を受信し、送信元認証手段903は、購入処理手段506から送信されたユーザID712を受信し、送信元のユーザを特定する。課金処理手段904は、受信された課金情報中に含まれる課金情報に従って、送信元認証手段903によって特定されたユーザに対して課金処理を行う。課金処理正常終了通知手段905は課金処理が正しく終了したことを示す、コンテンツの記録許可回数を書かれた権利情報を含む、課金処理正常終了通知713を購入処理手段506に送信する。配布元ユーザID取出し手段906は、課金情報711に配布元ユーザを特定するユーザIDが付加されているかどうかを判定し、付加されている場合には、そのユーザIDを取出し、配布元ユーザID復号手段907に、取出したユーザIDを復号化するように指示し、特典処理手段908に、復号化されたユーザIDによって特定されるユーザに対し、割引やクーポンの発効などの特

典処理を行うよう指示する。配布元ユーザID復号手段907は、配布元ユーザID取出し手段906の指示に従って、ユーザIDを復号化する。特典処理手段908は配布元ユーザID取出し手段906の指示に従って、特典処理を行う。

【0069】

以上のような、課金処理装置901の動作について、図15に示すフローチャートを用いて説明する。課金情報受信手段902は、購入処理手段506から送信された課金情報を受信し、送信元認証手段903は、購入処理手段506から送信されたユーザIDを受信する(S1501)。課金処理手段904は、送信元認証手段903によって受信されたユーザIDから特定されるユーザに対して、課金情報受信手段902によって受信された課金情報に含まれる課金制御情報に従って、課金処理を行う(S1502)。配布元ユーザID取出し手段は、課金処理受信手段902が受信した課金情報に、ユーザIDが付加されているかどうかを判定する(S1503)。付加されている場合には、配布元ユーザID復号手段907は、付加されているユーザIDを復号化し(S1504)、特典処理手段908は、S1504で復号化されたユーザIDによって特定されるユーザに対して、クーポンを与えるなどの特典処理を行う(S1505)。

【0070】

なお、ユーザIDの他に二次配付されるときにその二次配付の元となった、ソフトウェアおよび二次配付の媒体となった記録メディアのベンダーを識別する情報が記述されていた場合、課金サーバは各ベンダーに適切に利益がわたるよう処理する。

【0071】

以上で、本実施の形態で使用する課金処理装置901の説明を終わる。

【0072】

次に、本実施の形態におけるデジタルデータ再生装置105の説明を行う。

【0073】

図10は、本発明に係わるデジタルデータ再生装置のシステム構成図である。

【0074】

本発明のデジタルデータ再生装置 1 0 5 は、一般にはポータブル音響機器プレーヤのような民生機器によって実現され、入力読み取り手段 1 0 0 1、データ判別手段 1 0 0 2、データ読み取り手段 1 0 0 3、再生制御手段 1 0 0 4、復号手段 1 0 0 5、再生手段 1 0 0 6、外部出力手段 1 0 0 7 を備える。以後、これらの構成要素についての説明を行う。

【 0 0 7 5 】

なお、デジタルデータ再生装置 1 0 5 はポータブル音響機器プレーヤを想定しているが、据え置き型音響機器プレーヤ、PC など同様の構成要素をもつものであればよい。

【 0 0 7 6 】

入力読取り手段 1 0 0 1 は、記録メディアに記録されているコンテンツから再生するコンテンツを選択する等のユーザからの入力を受け取る。

【 0 0 7 7 】

データ読取り手段 1 0 0 3 は、入力読取り手段 1 0 0 1 が受け取った、ユーザからのコンテンツの選択を受信する。ユーザの選択したコンテンツの含まれたデジタルデータの再生制御情報を読取り、データ判別手段 1 0 0 2 に送る。データ判別手段 1 0 0 2 は、読取り手段 1 0 0 3 からデジタルデータの再生制御情報を受け取り、超流通形式のデータかどうかを判別し、判別結果をデータ読取り手段 1 0 0 3 に送る。

【 0 0 7 8 】

データ読取り手段 1 0 0 3 はコンテンツの再生制御情報を再生制御手段 1 0 0 4 に送り、再生制御手段 1 0 0 4 は再生制御情報から暗号化されたコンテンツの位置情報を取得する。データ読取り手段 1 0 0 3 は、再生制御手段 1 0 0 4 と、データ判別手段 1 0 0 2 の判別結果をもとに、暗号化されたコンテンツと、それを復号化する鍵を記録メディア 1 0 4 から読取り、コンテンツ復号手段 1 0 0 5 にそれぞれ送る。

【 0 0 7 9 】

再生手段 1 0 0 6 は再生制御情報を解釈する再生制御手段 1 0 0 4 の制御を受けながら、復号手段 1 0 0 5 より受取った、復号化したコンテンツをデコードし

、外部出力手段 1 0 0 7 に音声データを出力するように指示する。

【0 0 8 0】

以上のような、デジタルデータ再生装置 1 0 5 の動作について、図 1 6 に示すフローチャートを用いて説明する。

【0 0 8 1】

データ判別手段 1 0 0 2 は、ユーザが再生を要求するデジタルデータが超流通形式であるかどうかを、コンテンツの再生制御情報をもとに判別する（S 1 6 0 1）。超流通形式データである場合は、データ読取り手段 1 0 0 3 は記録メディア 1 0 4 のセキュアデータエリア 4 0 1 から、コンテンツを復号化する鍵を取出す（S 1 6 0 2）。超流通形式データではなく、記録メディア固有の ID を用いて暗号化されたコンテンツである場合は、記録メディア 1 0 4 から記録メディア固有の ID を取出す（S 1 6 0 5）。記録メディア固有の ID がコンテンツを解く鍵となる。これらコンテンツを解く鍵を利用して、コンテンツを復号化する（S 1 6 0 3）。復号化されたコンテンツを、コンテンツの再生制御情報を解釈する再生制御手段 1 0 0 4 の制御を受けながら、再生手段 1 0 0 6 がデコードし、外部出力手段 1 0 0 7 に音声出力の指示を出す（S 1 6 0 4）。

【0 0 8 2】

以上で本発明の第一の実施の形態の説明を終わる。

【0 0 8 3】

次に、本発明の第二の実施の形態の説明を行う。

【0 0 8 4】

（実施の形態 2）

本発明の実施の形態 2 のデジタルデータ記録装置は、実施の形態 1 のデジタルデータ記録再生装置の一部と同一の構成をとる。よって、同一の構成要素を同一の符号を用いて、説明する。

【0 0 8 5】

図 1 7 は実施の形態 2 におけるデジタルデータ記録装置 1 7 0 0 の構成を示す図である。

【0 0 8 6】

コンテンツサーバ 1 0 2、課金サーバ 1 0 3、および記録メディア 1 0 4 は実施の形態 1 で説明したコンテンツサーバ 1 0 2、課金サーバ 1 0 3、および記録メディア 1 0 4 と同一の構成であるため、説明を省略する。

【 0 0 8 7 】

実施の形態 2 におけるデジタルデータ記録装置 1 7 0 0 は、一般的にはデジタルデータ自動販売機で実現される。デジタルデータ自動販売機とは、小売店などに設置され、ユーザの用意した記録メディアもしくは、デジタルデータ自動販売機が用意した記録メディアに、ユーザが購入を希望するデジタルデータを記録して販売する機器である。ユーザ入力読取り手段 5 0 0、超流通形式データ受信手段 5 0 1、超流通形式データ記憶領域 5 0 2、データ取出し手段 5 0 3、配布元ユーザ ID 付加手段 5 0 4、コンテンツ記録手段 5 0 5、購入処理手段 5 0 6、セキュアデータ記憶領域 5 0 7、第一のデータ変換手段 5 1 2 から構成される。

【 0 0 8 8 】

各構成要素の果たす役割は実施の形態 1 における同一の符号のものと同一であるので、説明を省略する。

【 0 0 8 9 】

以上で本発明の第二の実施の形態の説明を終わる。

【 0 0 9 0 】

次に、本発明の第三の実施の形態の説明を行う。

【 0 0 9 1 】

(実施の形態 3)

図 1 8 は、本発明における、デジタルデータ記録再生装置 1 8 0 0 の構成を表わす図である。実施の形態 3 におけるデジタルデータ記録再生装置 1 8 0 0 は、実施の形態 1 のデジタルデータ再生装置 1 0 5 と、一部同一の構成を取るため、同一の構成要素については、同一の符号を付加して説明する。

【 0 0 9 2 】

実施の形態 3 におけるデジタルデータ記録再生装置 1 8 0 0 は、一般的には携帯電話で実現され、ユーザ入力読取り手段 1 8 0 2、データ受信手段 1 8 0 3

、コンテンツ記録手段1804、データ判別手段1002、データ読取り手段1003、再生制御手段1004、復号手段1005、再生手段1006、外部出力手段1007から構成される。

【0093】

ユーザ入力読取り手段1802は、サーバ1801から受信を希望するデジタルデータの受信指示や、記録メディア104に記録されているデジタルデータの再生指示などのユーザからの入力を読取る。

【0094】

データ受信手段1803は、ユーザ入力読取り手段1802から読取った、ユーザからの要求に基づいて、サーバ1801に送信を希望するコンテンツとそのデータ形式、ユーザを特定する情報の含まれた購入情報と、記録メディアIDを送る。そして、サーバから送信されてきたデジタルデータを受信し、コンテンツ記録手段1804に送る。

【0095】

コンテンツ記録手段1804は、データ受信手段1803からデジタルデータを受取り、超流通形式のデータであれば、記録メディア104の第一のエリア402に記録する。一方、記録メディアのIDを用いて暗号化されたデータであれば、記録メディア104の第二のエリア403に記録する。

【0096】

再生の動作については、実施の形態1における、デジタルデータ再生装置105と同一である。

【0097】

図19は、サーバ1801の構成を表わす図である。

【0098】

サーバ1801は、購入情報受信判別手段1903、記録メディアID受信手段1904、個人情報記憶領域1905、暗号手段1906、コンテンツ記憶領域1907、データ送信手段1908から構成される。

【0099】

購入情報受信判別手段1903は、デジタルデータ記録再生装置1800か

ら送信を希望するコンテンツとそのデータ形式が超流通形式かそうでないか、ユーザを特定する情報の含まれた購入情報1901を受取る。記録メディアID受信手段1904は記録メディアID1902を受信する。

【0100】

購入情報1901に書かれた、ユーザが受信を希望するデジタルデータのデータ形式が、超流通形式のデータである場合、暗号手段1906はコンテンツ記憶領域1907からユーザが希望したコンテンツと、それを暗号化する鍵、課金情報を取り出して、超流通形式のデータを作成する。また、ユーザが受信を希望するデータ形式が、超流通形式のデータでない場合、記録メディアID受信手段1904は記録メディア104から固有のIDを受信し、受信した記録メディアID1902を利用して、コンテンツを暗号化する。

【0101】

記録メディア104への記録を行うデジタルデータ記録再生装置1800でなく、サーバ1801でデジタルデータの暗号化を行うのは、デジタルデータ記録再生装置1800が一般的には携帯電話で実現され、より安価に実現するために、暗号化手段を持たない構成が考えられるからである。

【0102】

データ送信手段1908は暗号手段1906から受取ったデジタルデータを、デジタルデータ記録再生装置1800へ送信する。

【0103】

以上で本発明の第三の実施の形態の説明を終わる。

【0104】

次に、本発明の第四の実施の形態の説明を行う。

【0105】

(実施の形態4)

本発明の実施の形態4のデジタルデータ記録再生装置について説明する。

【0106】

図20は実施の形態4におけるデジタルデータ記録装置2000の構成を示す図である。

【0 1 0 7】

記録メディア 1 0 4 は実施の形態 1 で説明した記録メディア 1 0 4 と同一の構成であるため、説明を省略する。

【0 1 0 8】

実施の形態 4 におけるデジタルデータ記録再生装置 2 0 0 0 は、一般的にはラジカセ、コンポーネントステレオ機器のような、据え置き型民生機器で実現され、ユーザ入力読取り手段 2 0 0 1、デジタルデータ読取り手段 2 0 0 2、デジタルデータ記憶領域 2 0 0 3、データ取出し手段 2 0 0 4、配布元ユーザ ID 付加手段 2 0 0 5、コンテンツ記録手段 2 0 0 6、セキュアデータ記憶領域 2 0 0 7、データ判別手段 2 0 0 8、再生制御手段 2 0 0 9、コンテンツ復号手段 2 0 1 0、再生手段 2 0 1 1、外部出力手段 2 0 1 2 から構成される。また、デジタルデータ記録装置 2 0 0 0 は、機器固有の ID を持ち、これはセキュアデータ記憶領域 2 0 0 7 に記録される。

【0 1 0 9】

ユーザ入力読取り手段 2 0 0 1 は、具体的にはリモコンなどで実現され、記録メディア 1 0 4 のデジタルデータの再生要求、デジタルデータ記憶領域 2 0 0 3 に記録されたデジタルデータの再生要求、記録メディア 1 0 4 へのデジタルデータの記録要求といったユーザからの入力を読取る。

【0 1 1 0】

デジタルデータ読取り手段 2 0 0 2 は、ユーザ入力読取り手段 2 0 0 1 から読取ったユーザからの要求に基づいて、記録メディア 1 0 4 からデジタルデータを読取る。このとき、記録メディアから読取るデータの形式は、第一の超流通形式データ 2 3 0 か、第二の超流通形式データ 3 2 0 である。デジタルデータ読取り手段は記録メディア 1 0 4 から読取ったデジタルデータを、デジタルデータ記憶領域 2 0 0 3 に記録するが、このとき記録するデータ形式は、第一の超流通形式 2 3 0、第二の超流通形式 3 2 0、または機器固有の ID により暗号化されたもののいずれであってもよい。このとき、機器固有 ID により暗号化されたものを記録する場合は、超流通形式のデータ形式から機器固有 ID で暗号化されたデータ形式にデータ形式を変換しなければならない。また、デジタルデータ読

取り手段 2 0 0 2 は記録メディア 1 0 4 のセキュアデータエリアに記録された、コンテンツの記録許可回数が記述された権利情報を取出し、セキュアデータ記憶領域 2 0 0 7 に記録する。

【 0 1 1 1 】

デジタルデータ記憶領域 2 0 0 3 には、前述のとおり、第一の超流通形式 2 3 0、第二の超流通形式 3 2 0、および機器固有の ID を用いて暗号化された形式のデータが記録されるが、デジタルデータ記録再生装置 2 0 0 0 がこのデータ形式全てを記録・再生する手段を備えておく必要はない。

【 0 1 1 2 】

配布元ユーザ ID 付加手段 2 0 0 5、コンテンツ記録手段 2 0 0 6、セキュアデータ記憶領域 2 0 0 7 による第一の超流通形式 2 3 0 から第二の超流通形式 3 2 0 に変換して、記録する動作は、実施の形態 1 に示される、配布元ユーザ ID 付加手段 5 0 4、コンテンツ記録手段 5 0 5、セキュアデータ記憶領域 5 0 7 による動作と同一であるため、説明を省略する。

【 0 1 1 3 】

データ取出し手段 2 0 0 4 は、入力読取り手段 2 0 0 1 が読取った、ユーザからの入力に基づいて、デジタルデータ記憶領域 2 0 0 3 よりデジタルデータの再生制御情報を取出す。データ取出し手段 2 0 0 4 は取出した再生制御情報をデータ判別手段 2 0 0 8 に送り、データ判別手段 2 0 0 8 は受取った再生制御情報から、超流通形式のデータかどうかを判別し、判別結果をデータ取出し手段 2 0 0 4 に送る。

【 0 1 1 4 】

データ取出し手段 2 0 0 4 は再生制御情報を再生制御手段 2 0 0 9 へ送り、再生制御手段 2 0 0 9 は再生制御情報から暗号化されたコンテンツの位置情報を取得する。再生制御手段 2 0 0 9 が得たコンテンツの位置情報と、データ判別手段 2 0 0 8 の判別結果をもとに、暗号化されたコンテンツと、その鍵をコンテンツ復号手段 2 0 1 0 へそれぞれ送る。

【 0 1 1 5 】

コンテンツ復号手段 2 0 1 0 は受取った暗号化されたコンテンツを復号化する

。再生手段 2 0 1 1 はコンテンツの再生制御情報を解釈する再生制御手段 2 0 0 9 の制御を受けながら、コンテンツ復号手段 2 0 1 0 より受取った、復号化されたコンテンツをデコードし、外部出力手段 2 0 1 2 に音声データを出力するように指示する。

【0 1 1 6】

以上のような、デジタルデータ記録再生装置 2 0 0 0 のデジタルデータ記憶領域に記録されたデジタルデータの再生動作について、図 2 1 に示すフローチャートを用いて説明する。

【0 1 1 7】

ユーザ入力読取り手段 2 0 0 1 は、ユーザから再生すべきコンテンツ選択の入力を読取り（S 2 1 0 0）、データ取出し手段 2 0 0 4 に送る。データ取出し手段 2 0 0 4 はユーザ読取り手段 2 0 0 1 から送られてきた情報をもとに、デジタルデータ記憶領域 2 0 0 3 からデジタルデータの再生制御情報を読取り、データ判別手段 2 0 0 8 に送る。データ判別手段 2 0 0 8 は、ユーザが再生を要求しているコンテンツを含むデジタルデータが超流通形式であるかどうかを判別する（S 2 1 0 1）。超流通形式データである場合は、コンテンツ復号手段 2 0 1 0 は、セキュアデータ記憶領域 2 0 0 7 からコンテンツを復号化する鍵を受取り（S 2 1 0 2）、データ取出し手段から暗号化されたコンテンツを受取る（S 2 1 0 4）。デジタルデータ記憶領域 2 0 0 3 から取出したデータが超流通形式データではなく、機器固有の ID を用いて暗号化されたコンテンツである場合は、セキュアデータ記憶領域 2 0 0 7 より、機器固有の ID を取得する（S 2 1 0 3）。この ID がコンテンツを解く鍵となる。これらコンテンツを解く鍵を利用して、コンテンツを復号化する（S 2 1 0 5）。再生手段 2 0 1 1 は再生制御情報を解釈する再生制御手段 2 0 0 9 の制御を受けながら、復号化されたコンテンツをデコードし、外部出力手段 2 0 1 2 に音声出力の指示を出す（S 2 1 0 6）。

【0 1 1 8】

次にデジタルデータ記録再生装置 2 0 0 0 が記録メディア 1 0 4 に記録されたデジタルデータを再生する動作について説明する。フローチャートはディジ

タルデータ記憶領域から再生するときと同じ図 21 を用いる。

【0119】

データ判別手段 2008 は、データ取出し手段 2004 が記録メディア 104 から読取ったデータが超流通形式であるかどうかを判別する (S2101)。超流通形式データである場合は、データ取出し手段 2004 は記録メディア 104 のセキュアデータエリア 401 から、コンテンツを復号化する鍵を取出す (S2102)。超流通形式データではなく、記録メディア固有の ID を用いて暗号化されたコンテンツである場合は、記録メディア 104 から記録メディア固有の ID を取出す (S2103)。記録メディア固有の ID がコンテンツを解く鍵となる。これらコンテンツを解く鍵を利用して、コンテンツを復号化する (S1105)。復号化されたコンテンツを、再生制御手段 2009 に基づいて再生手段 2011 がデコードし、外部出力手段 2012 に音声出力の指示を出す (S2106)。

【0120】

【発明の効果】

以上説明したように、本発明の記録メディアによれば、記録メディア固有の ID により暗号化されたデータと、超流通形式のデータを同時に記録することができ、記録メディアを用いた、超流通の仕組みを実現することが可能となる。

【0121】

具体的には、二次配信元となるユーザはインターネット等からダウンロードする音楽コンテンツを、第 1 の超流通形式のデータのまま記録メディアに記録することができる。また、記録メディアの ID を鍵としたコンテンツ暗号形式であっても、二次配信が可能な仕組みで記録メディアに記録することが可能である。

【0122】

記録メディアにより二次配信された第 1 の超流通形式の音楽コンテンツや記録メディアの ID を鍵とした暗号形式のコンテンツは、二次配信を受けたユーザが課金処理を行うことができる。また、コンテンツ暗号データに変換された音楽コンテンツは、再生装置により復号化され再生されることが可能になる。これにより、記録メディアを介した二次配信が可能になり、かつ、二次配信された音楽コン

テンツに対しても課金処理が行えるため音楽コンテンツの著作権が保護される。

【0 1 2 3】

また、本発明のデジタルデータ記録装置によれば、インターネットを通じて、もしくは記録メディアから受信した第一の超流通形式のデータを、自らが備える超流通形式データ記憶領域に記録しておくことができ、その超流通形式データ記憶領域 5 0 2 にある第一の超流通形式データ 2 3 0 に、ユーザを特定できる情報を配布元ユーザ ID として付与し、第二の超流通形式データ 3 2 0 として、記録メディアに記録することができる。

【0 1 2 4】

また、本発明のデジタルデータ記録再生装置によれば、記録メディアから課金処理済みの超流通形式のデータをアップロードして、自らが備えるデジタルデータ記憶領域に記録・管理することができる。

【0 1 2 5】

また、本発明の課金処理装置によれば、第二の超流通形式のデータが記録された記録メディアを受取った第三者が、そのデータを購入した場合、配布元のユーザは何らかのメリットを享受することができる。これにより、ユーザがより積極的に第二の超流通形式データ 3 2 0 を作成、配付し、超流通を促進させるという効果がある。

【0 1 2 6】

また、本発明の再生装置によれば、記録メディア固有の ID で暗号化されたデータと、超流通形式のデータの両方のデータを、それぞれが記録されている記録メディアから再生することができる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態 1 における各装置の関係図

【図 2】

第一の超流通形式データのデータ構造を示す図

【図 3】

第二の超流通形式データのデータ構造を示す図

【図 4】

記録メディアの構成を示す図

【図 5】

デジタルデータ記録再生装置の構成を示す図

【図 6】

配布元ユーザ ID 付加手段の構成を示す図

【図 7】

購入処理手段の構成を示す図

【図 8】

課金処理情報の一例を示す図

【図 9】

課金処理装置の構成を示す図

【図 10】

デジタルデータ再生装置の構成を示す図

【図 11】

デジタルデータ記録再生装置の受信データ記録の動作を示すフローチャート

【図 12】

デジタルデータ記録再生装置の第一の超流通形式データから第二の超流通形式データを作成する動作を示すフローチャート

【図 13】

デジタルデータ記録再生装置の購入処理の動作を示すフローチャート

【図 14】

デジタルデータ記録再生装置の再生の動作を示すフローチャート

【図 15】

課金処理装置の動作を示すフローチャート

【図 16】

デジタルデータ再生装置の動作を示すフローチャート

【図 17】

本発明の実施の形態 2 におけるデジタルデータ記録装置の構成を示す図

【図 1 8】

本発明の実施の形態 3 におけるデジタルデータ記録再生装置の構成を示す図

【図 1 9】

サーバの構成を示す図

【図 2 0】

本発明の実施の形態 4 におけるデジタルデータ記録再生装置の構成を示す図

【図 2 1】

デジタルデータ記録再生装置の動作を示すフローチャート

【符号の説明】

- 1 0 1 (a) デジタルデータ記録再生装置
- 1 0 1 (b) デジタルデータ記録再生装置
- 1 0 1 (c) デジタルデータ記録再生装置
- 1 0 2 コンテンツサーバ
- 1 0 3 課金サーバ
- 1 0 4 記録メディア
- 1 0 5 デジタルデータ再生装置
- 2 0 1 鍵
- 2 0 2 課金情報
- 2 0 3 データ
- 2 0 4 コンテンツ
- 2 1 0 暗号化ヘッダ部
- 2 2 0 暗号化コンテンツ部
- 2 3 0 第一の超流通形式データ
- 3 0 1 ユーザ I D
- 3 1 0 暗号化 I D 部
- 3 2 0 第二の超流通形式データ
- 4 0 1 セキュアデータエリア
- 4 0 2 第一のエリア
- 4 0 3 第二のエリア

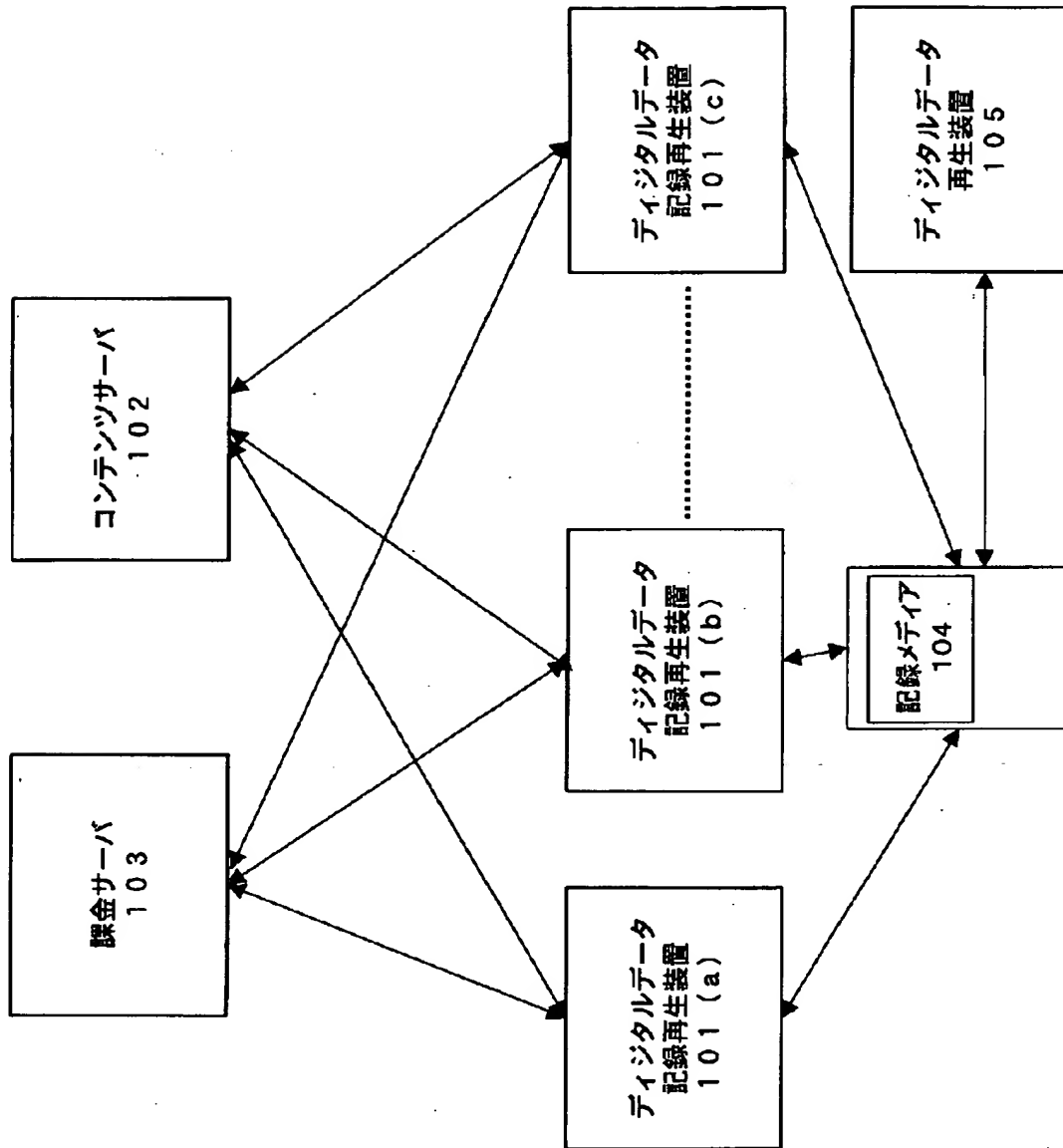
- 5 0 0 ユーザ入力読み取り手段
- 5 0 1 超流通形式データ受信手段
- 5 0 2 超流通形式データ記憶領域
- 5 0 3 データ取出し手段
- 5 0 4 配布元ユーザ I D 付加手段
- 5 0 5 コンテンツ記録手段
- 5 0 6 購入処理手段
- 5 0 7 セキュアデータ記憶領域
- 5 0 8 コンテンツ復号手段
- 5 0 9 再生制御手段
- 5 1 0 再生手段
- 5 1 1 外部出力手段
- 5 1 2 第一のデータ形式変換手段
- 5 1 3 第二のデータ形式変換手段
- 6 0 1 ユーザ I D 取得手段
- 6 0 2 ユーザ I D 暗号化手段
- 6 0 3 配布元ユーザ I D 結合手段
- 7 0 1 暗号化ヘッダ部取出し手段
- 7 0 2 課金情報取出し手段
- 7 0 3 配布元ユーザ I D 取出し手段
- 7 0 4 配布元ユーザ I D 付加手段
- 7 0 5 課金情報送信手段
- 7 0 6 送信元ユーザ I D 送信手段
- 7 0 7 課金処理正常終了受信手段
- 7 0 8 コンテンツ鍵取出し手段
- 7 0 9 コンテンツ鍵書き込み手段
- 7 1 0 超流通形式データ
- 7 1 1 課金情報
- 7 1 2 ユーザ I D

- 7 1 3 課金処理正常終了通知
- 7 1 4 権利情報書き込み手段
- 8 0 1 ユーザ I D
- 8 0 2 課金情報
- 9 0 1 課金処理装置
- 9 0 2 課金情報受信手段
- 9 0 3 送信元認証手段
- 9 0 4 課金処理手段
- 9 0 5 課金処理正常終了通知手段
- 9 0 6 配布元ユーザ I D 取出し手段
- 9 0 7 配布元ユーザ I D 復号手段
- 9 0 8 特典処理手段
- 1 0 0 1 入力読取り手段
- 1 0 0 2 データ判別手段
- 1 0 0 3 データ読取り手段
- 1 0 0 4 再生制御手段
- 1 0 0 5 復号手段
- 1 0 0 6 再生手段
- 1 0 0 7 外部出力手段
- 1 7 0 0 デジタルデータ記録装置
- 1 8 0 0 デジタルデータ記録再生装置
- 1 8 0 1 サーバ
- 1 8 0 2 ユーザ入力読取り手段
- 1 8 0 3 データ受信手段
- 1 8 0 4 コンテンツ記録手段
- 1 9 0 1 購入情報
- 1 9 0 2 記録メディア I D
- 1 9 0 3 購入情報受信判別手段
- 1 9 0 4 記録メディア I D 受信手段

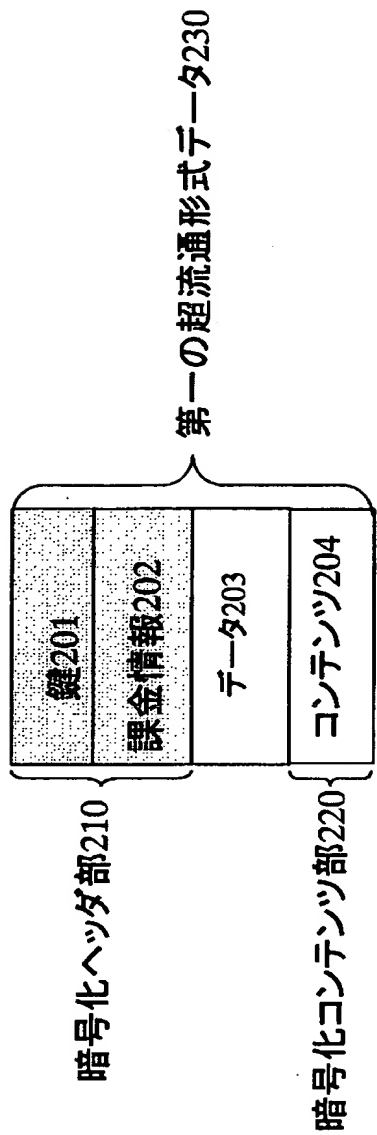
- 1 9 0 5 個人情報記憶領域
- 1 9 0 6 暗号手段
- 1 9 0 7 コンテンツ記憶領域
- 1 9 0 8 データ送信手段
- 2 0 0 0 デジタルデータ記録再生装置
- 2 0 0 1 ユーザ入力読取り手段
- 2 0 0 2 デジタルデータ読取り手段
- 2 0 0 3 デジタルデータ記憶領域
- 2 0 0 4 データ取出し手段
- 2 0 0 5 配布元ユーザID付加手段
- 2 0 0 6 コンテンツ記録手段
- 2 0 0 7 セキュアデータ記憶領域
- 2 0 0 8 データ判別手段
- 2 0 0 9 再生制御手段
- 2 0 1 0 コンテンツ復号手段
- 2 0 1 1 再生手段
- 2 0 1 2 外部出力手段

【書類名】 図面

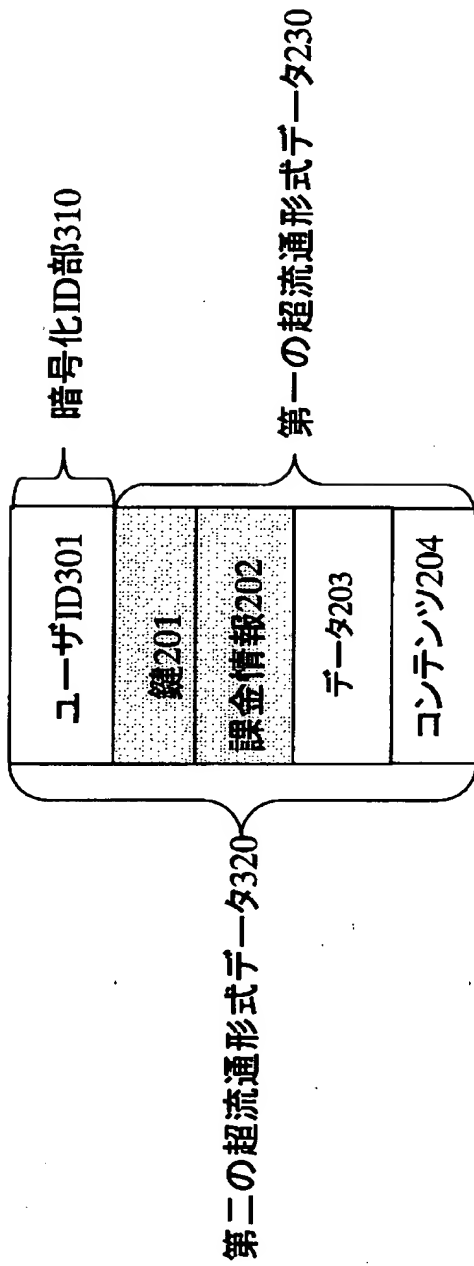
【図 1】



【図 2】



【図 3】

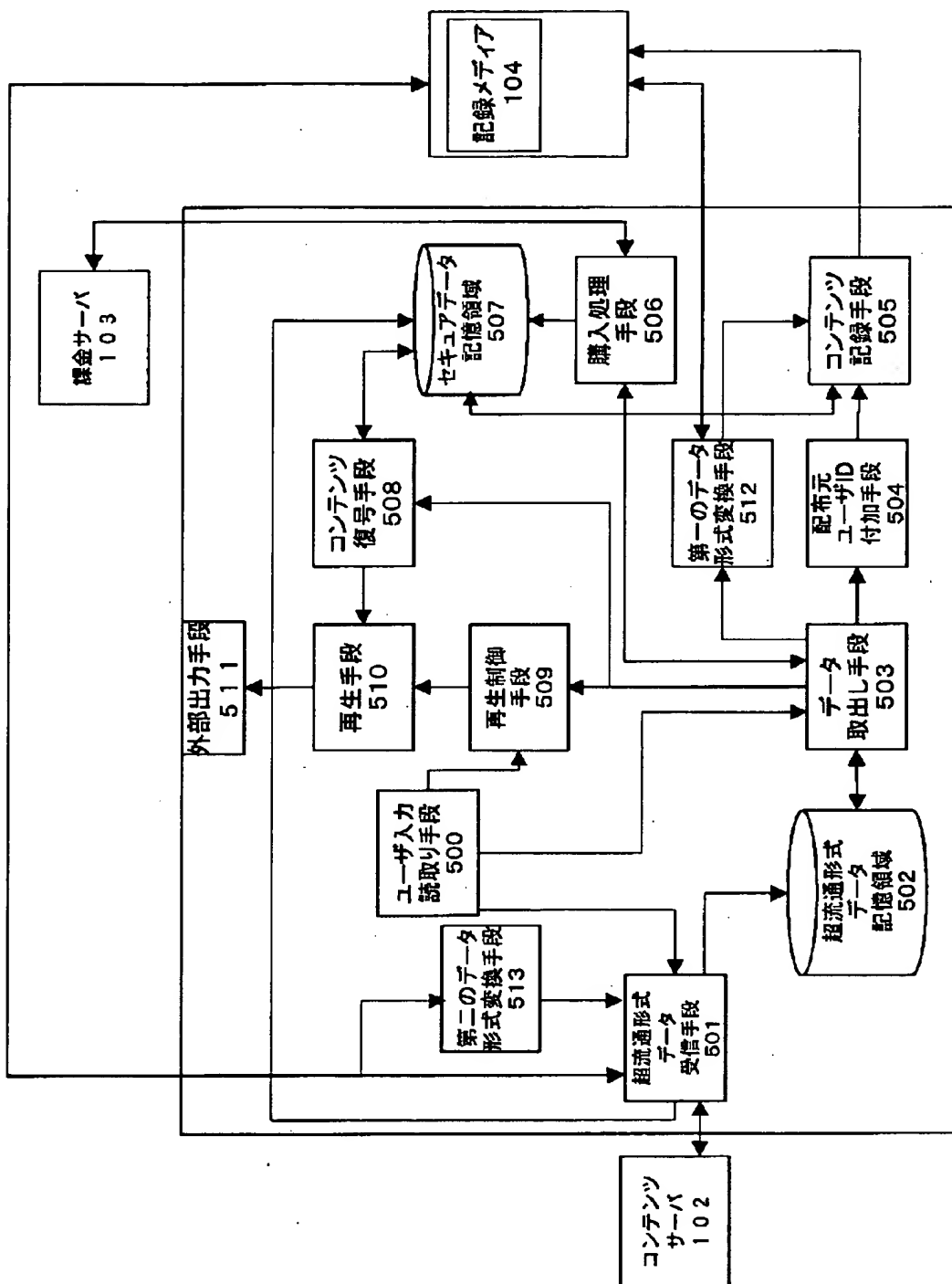


【図 4】

記録メディア104

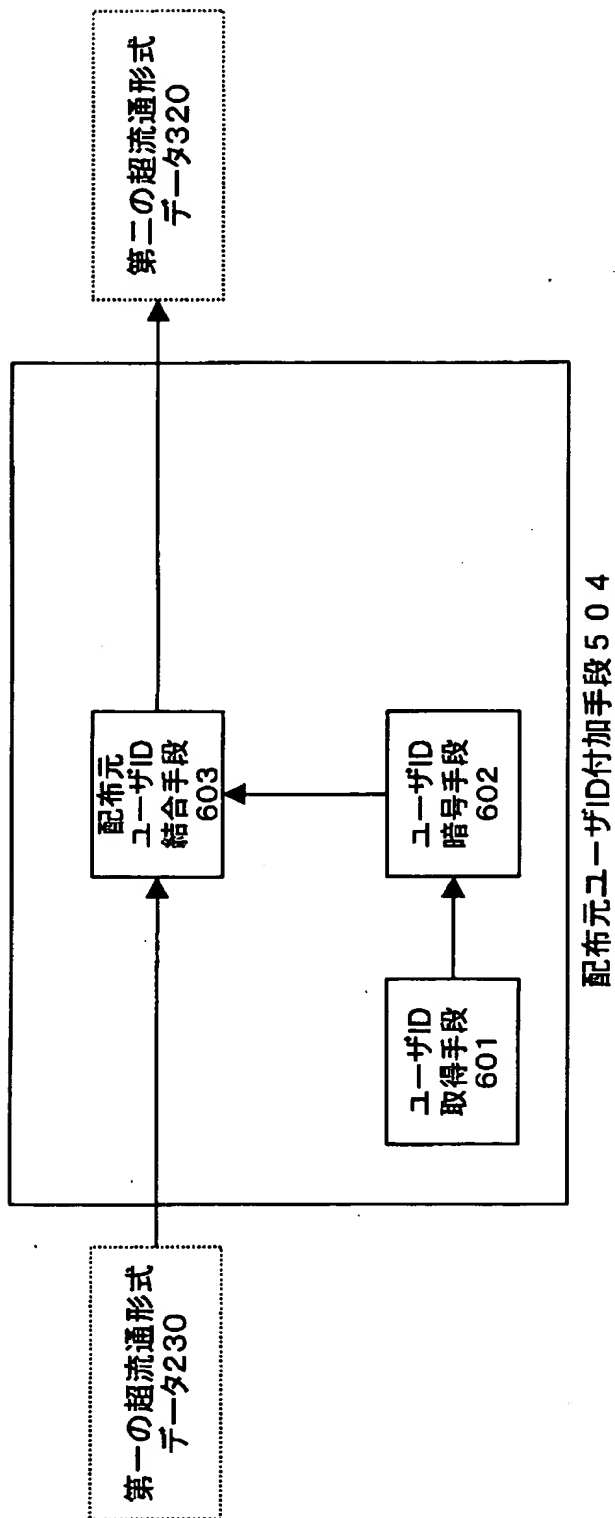
セキュアデータエリア401
第一のエリア402 超流通形式のデータ が格納される
第二のエリア403 超流通形式以外のデータ が格納される

【図 5】

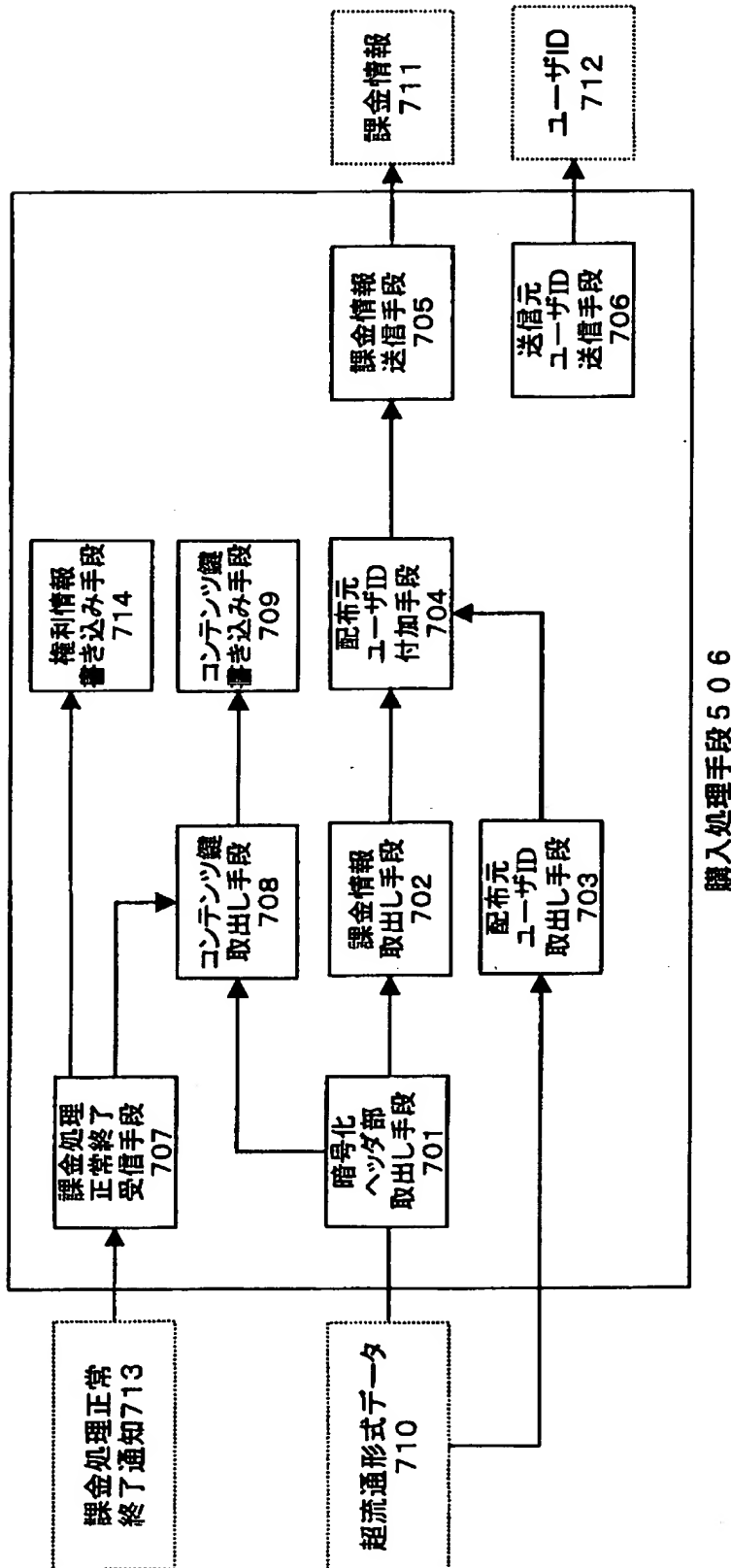


デジタルデータ記録再生装置101(a)

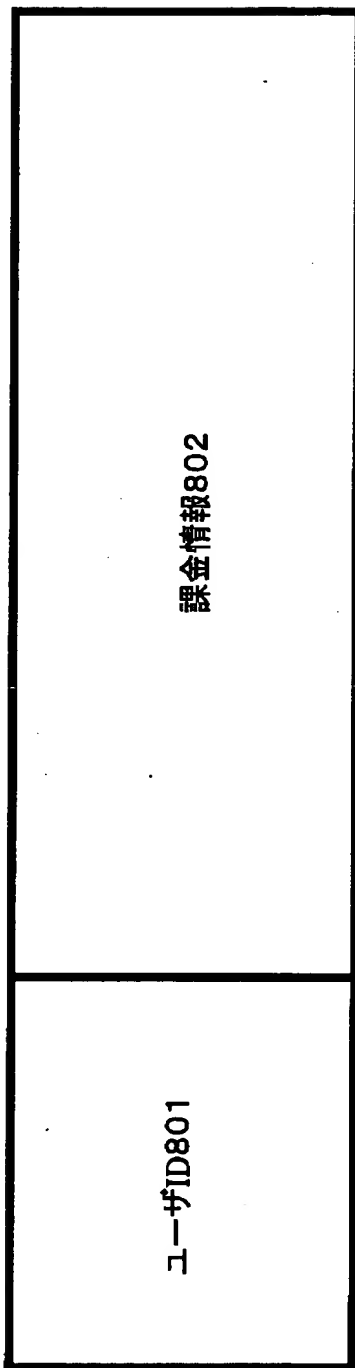
【図 6】



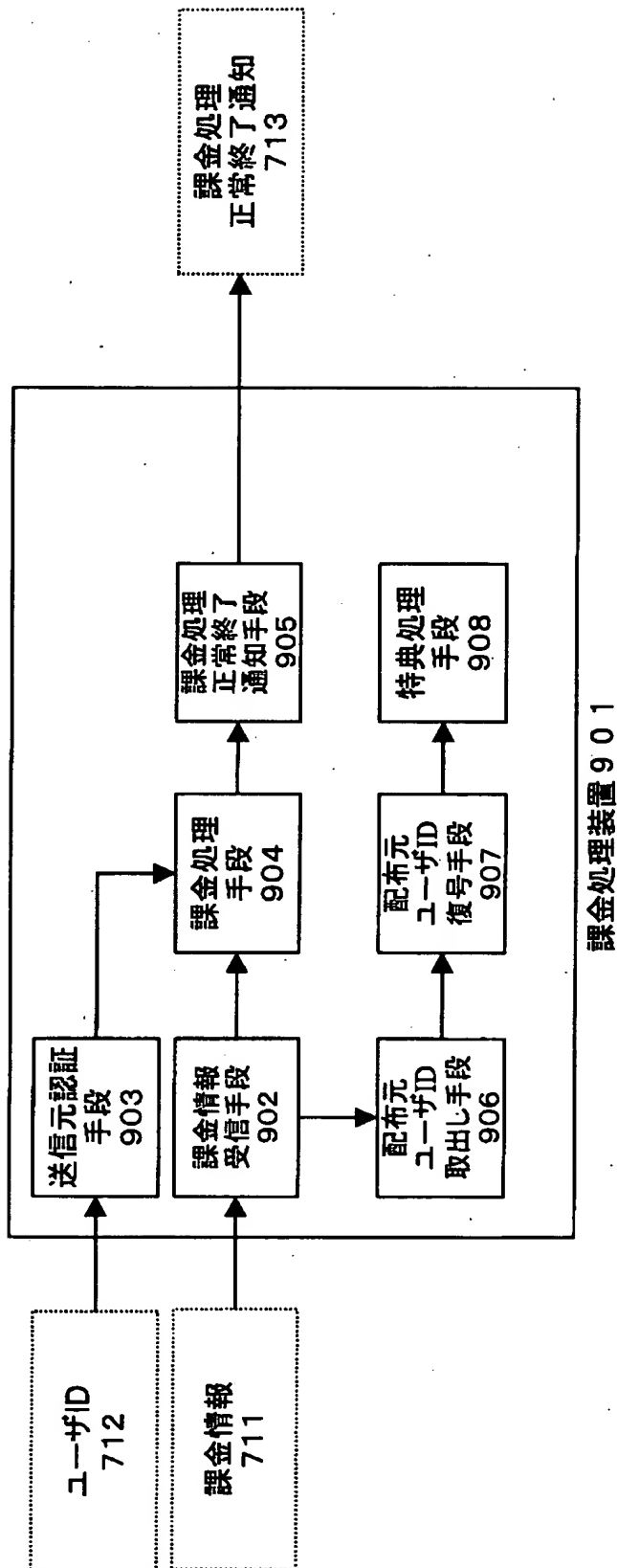
【図 7】



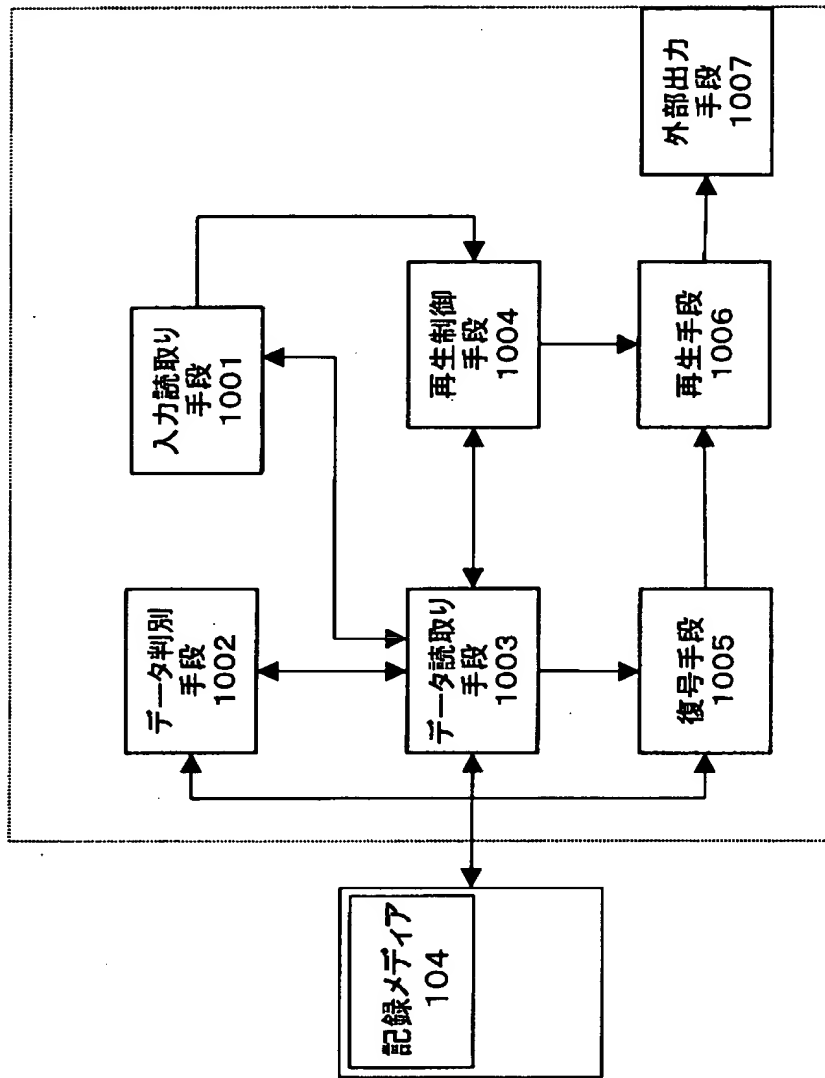
【図 8】



【図 9】

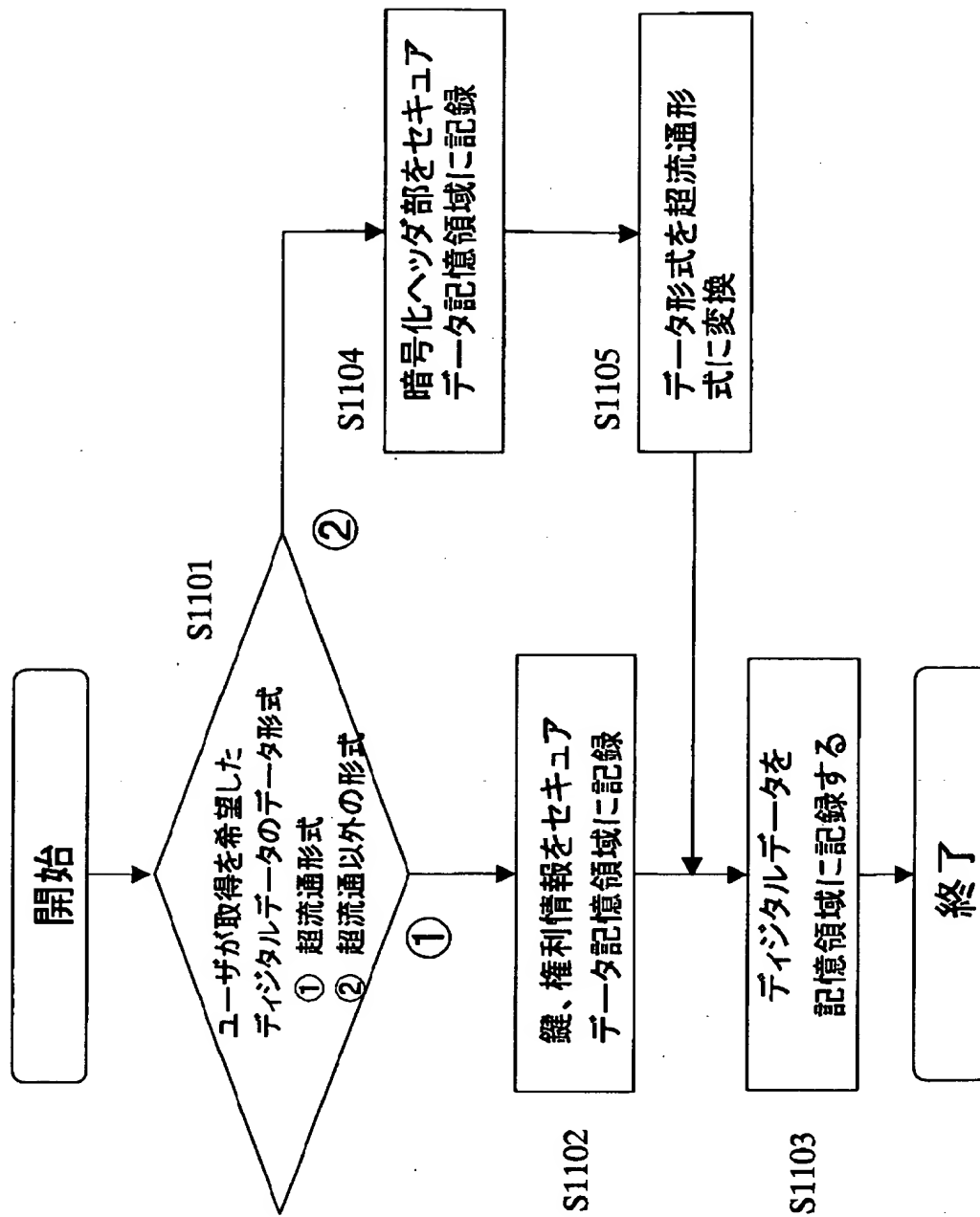


【図 1 0】

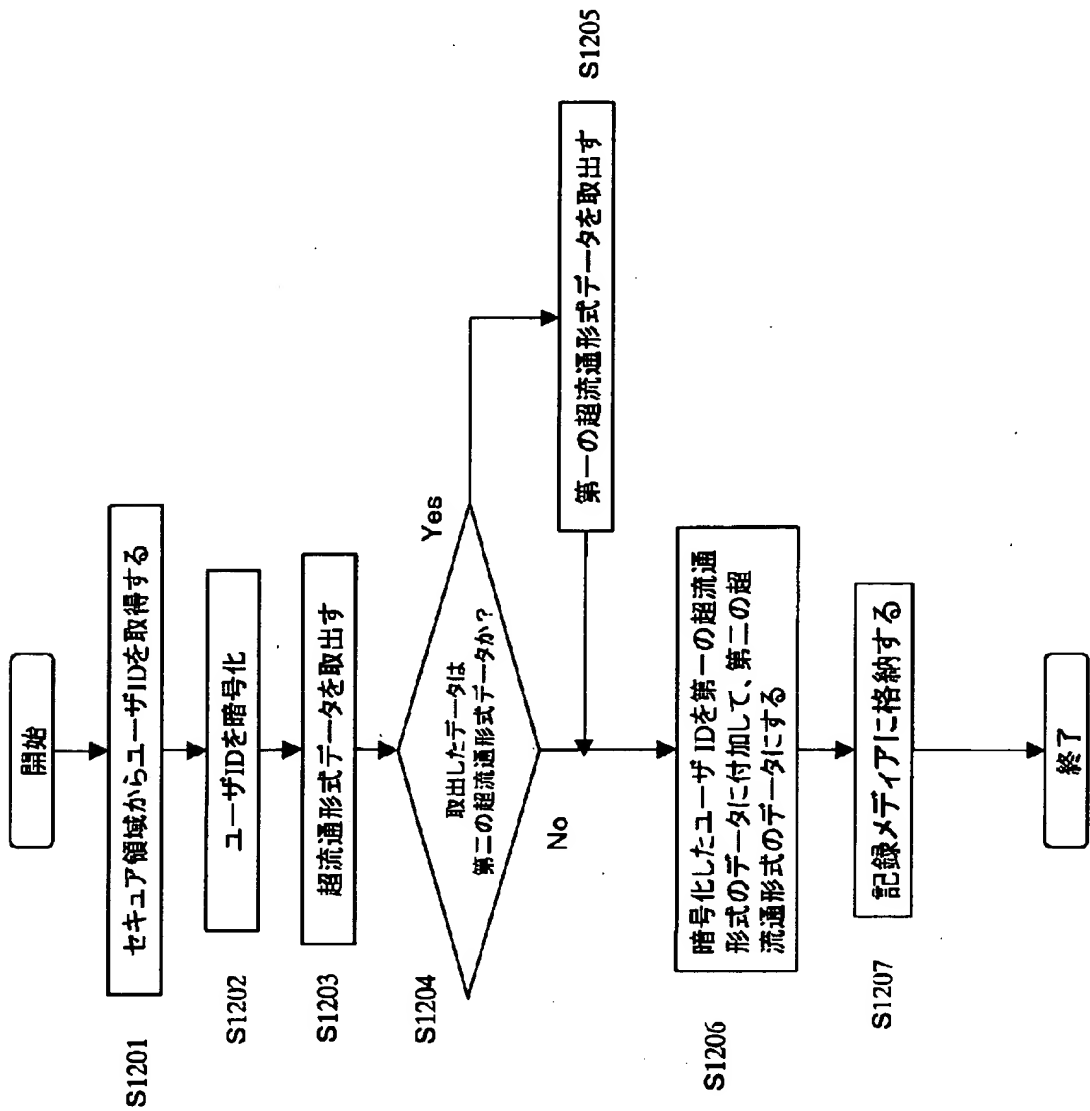


デジタルデータ再生装置105

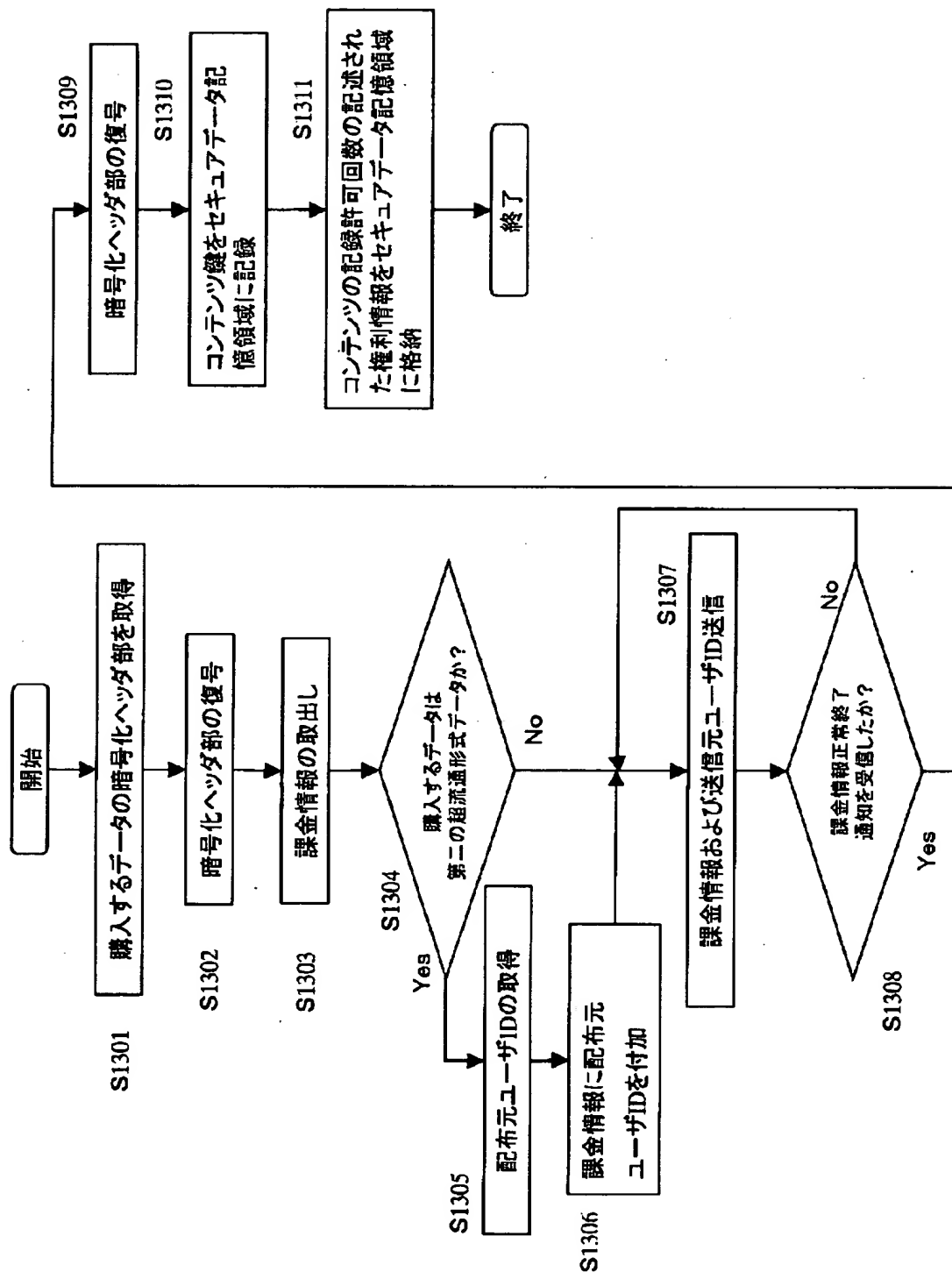
【図 1 1】



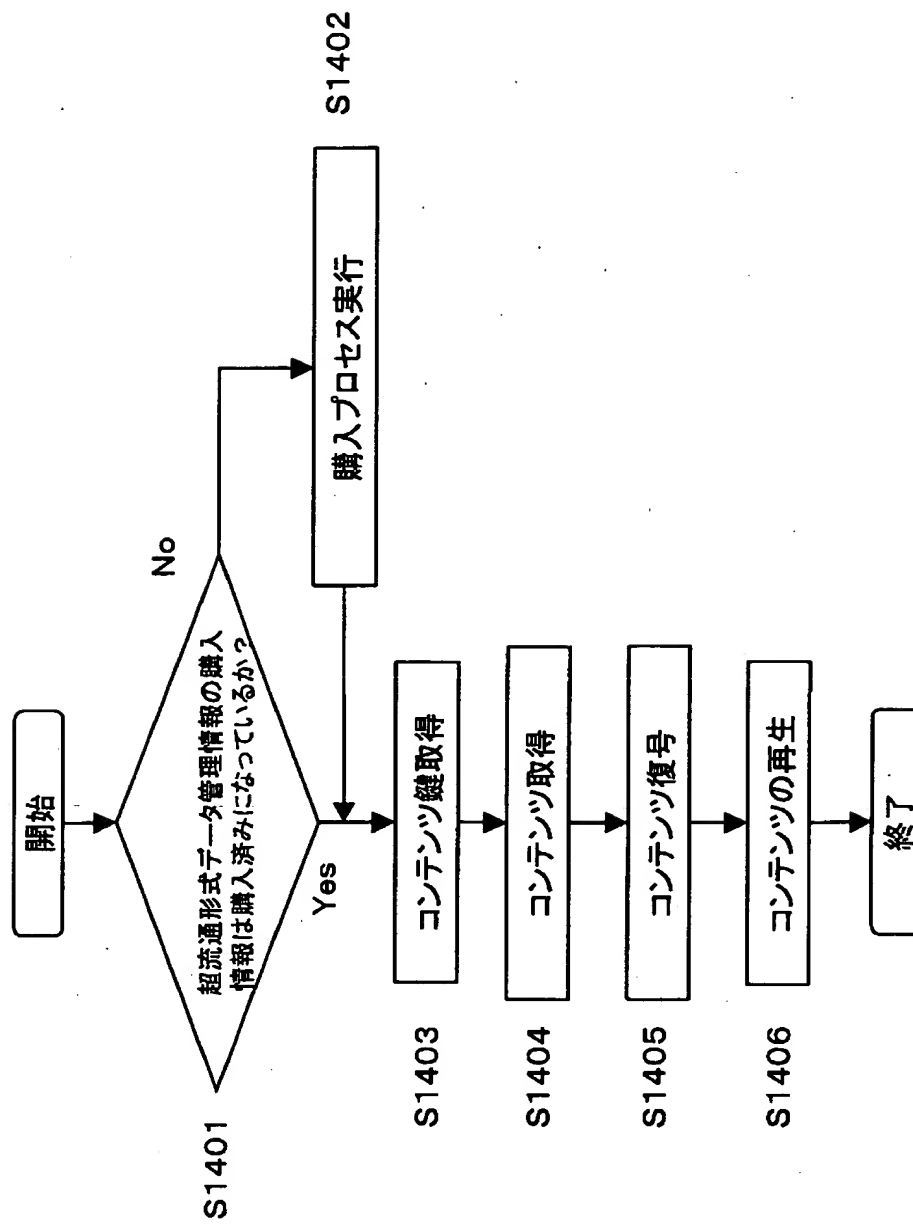
【図 1 2】



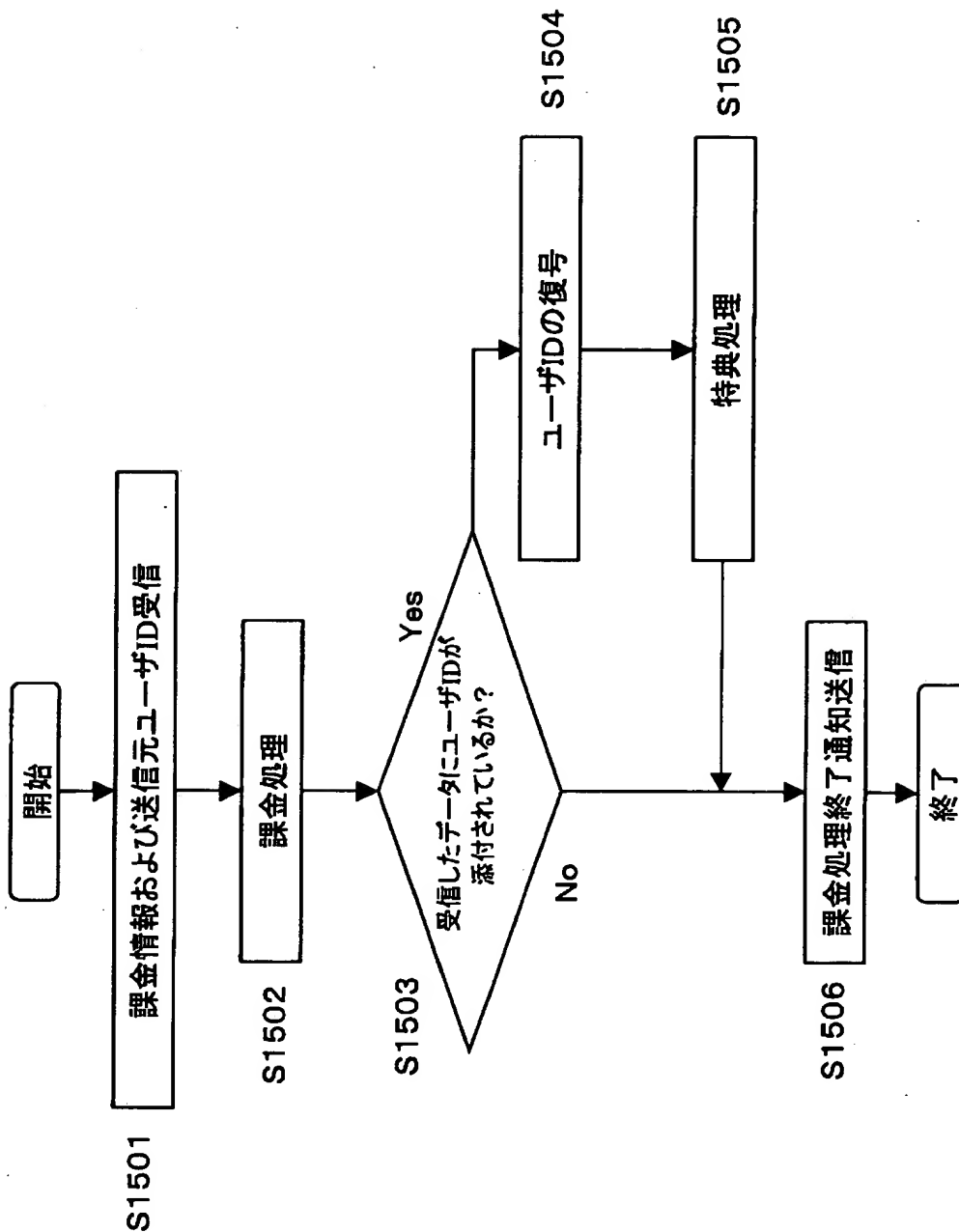
【図 1 3】



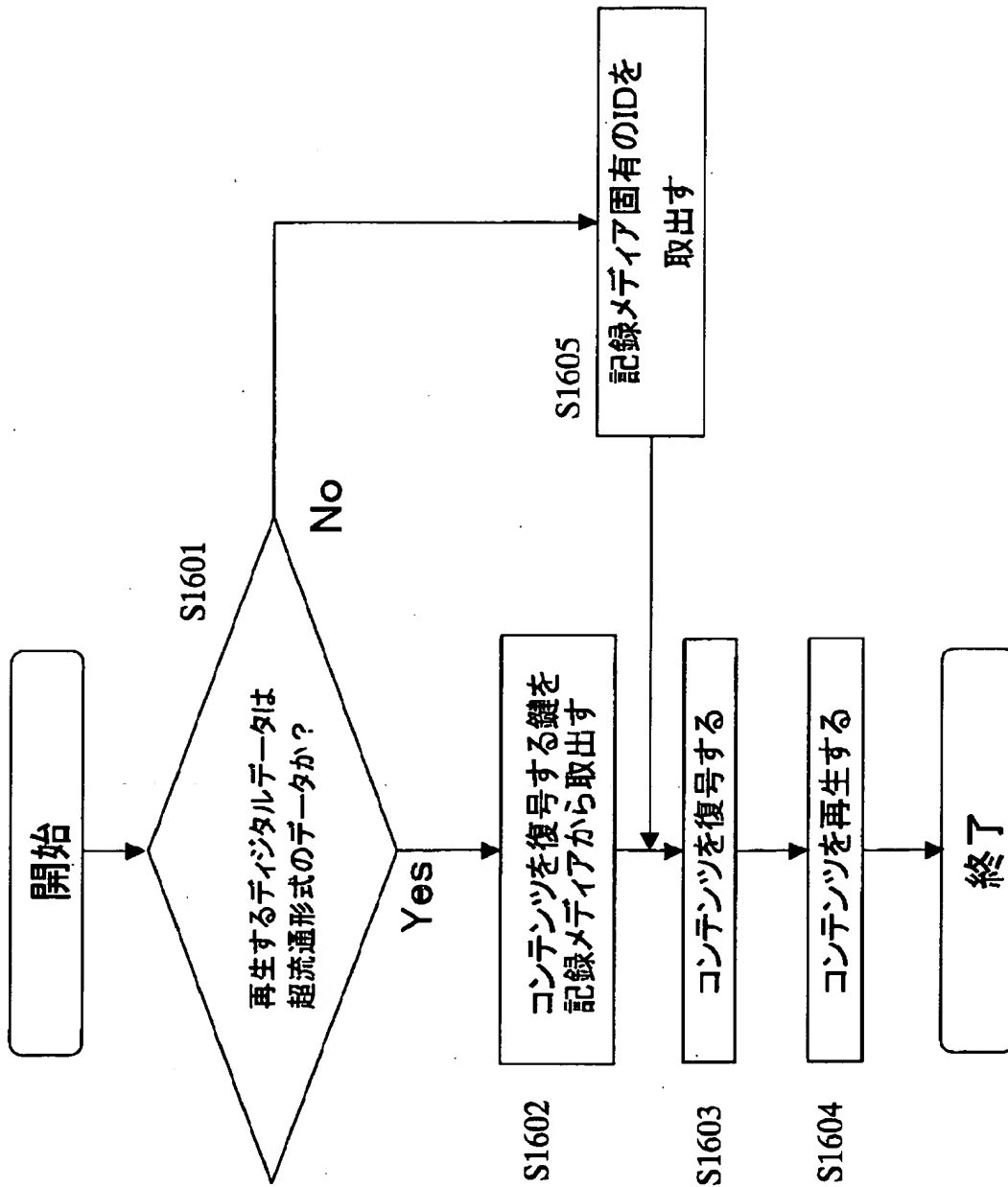
【図 1 4】



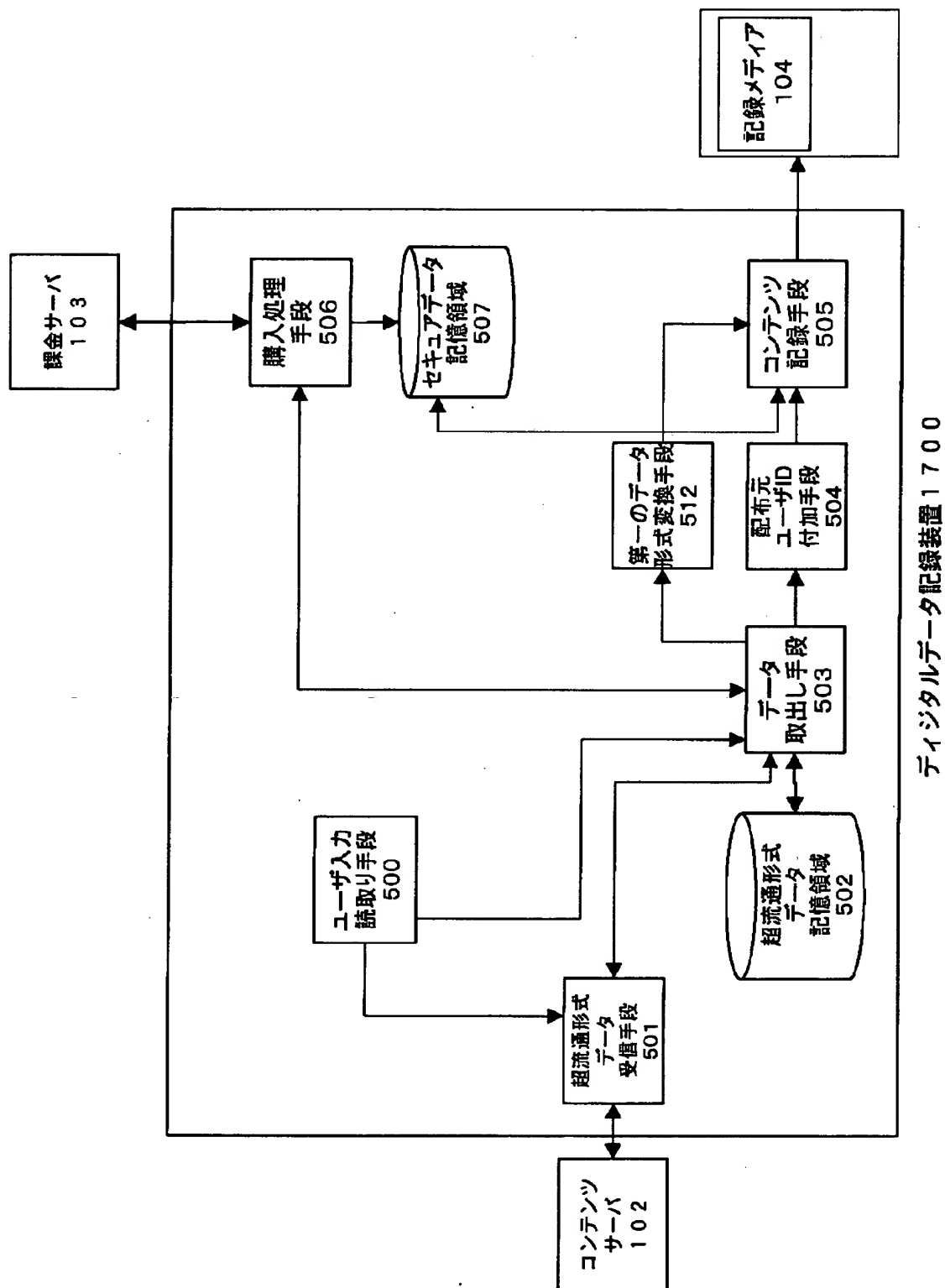
【図 1 5】



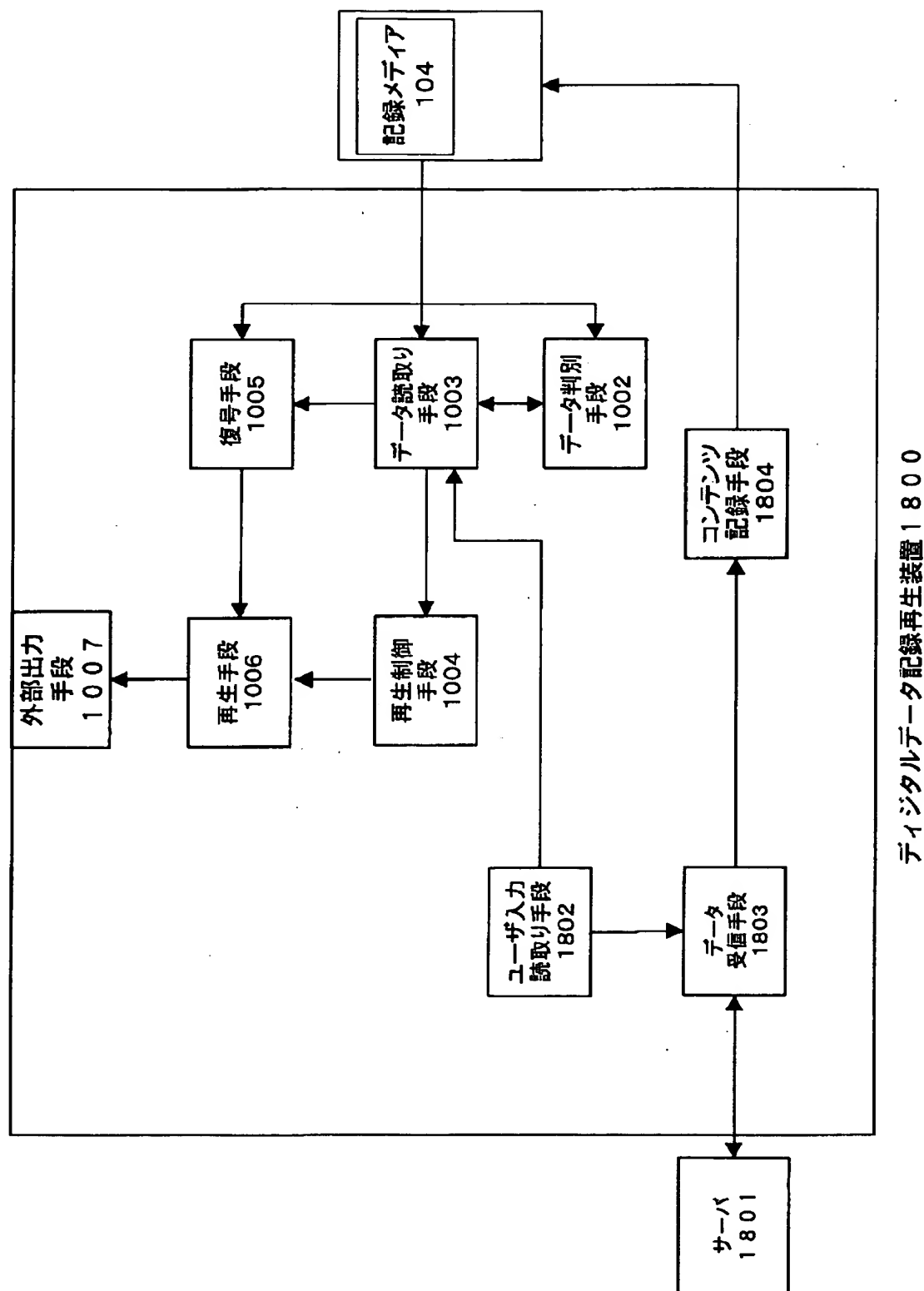
【図 1 6】



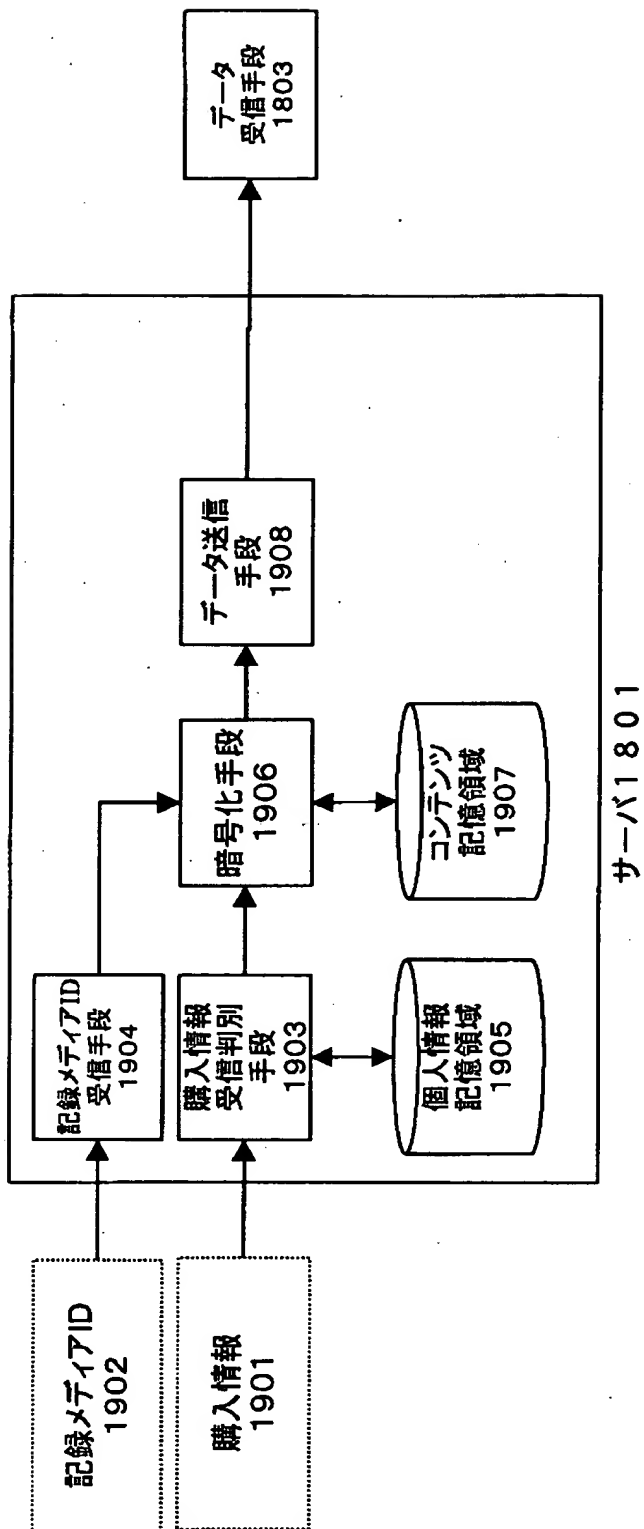
【図 1 7】



【図 1 8】

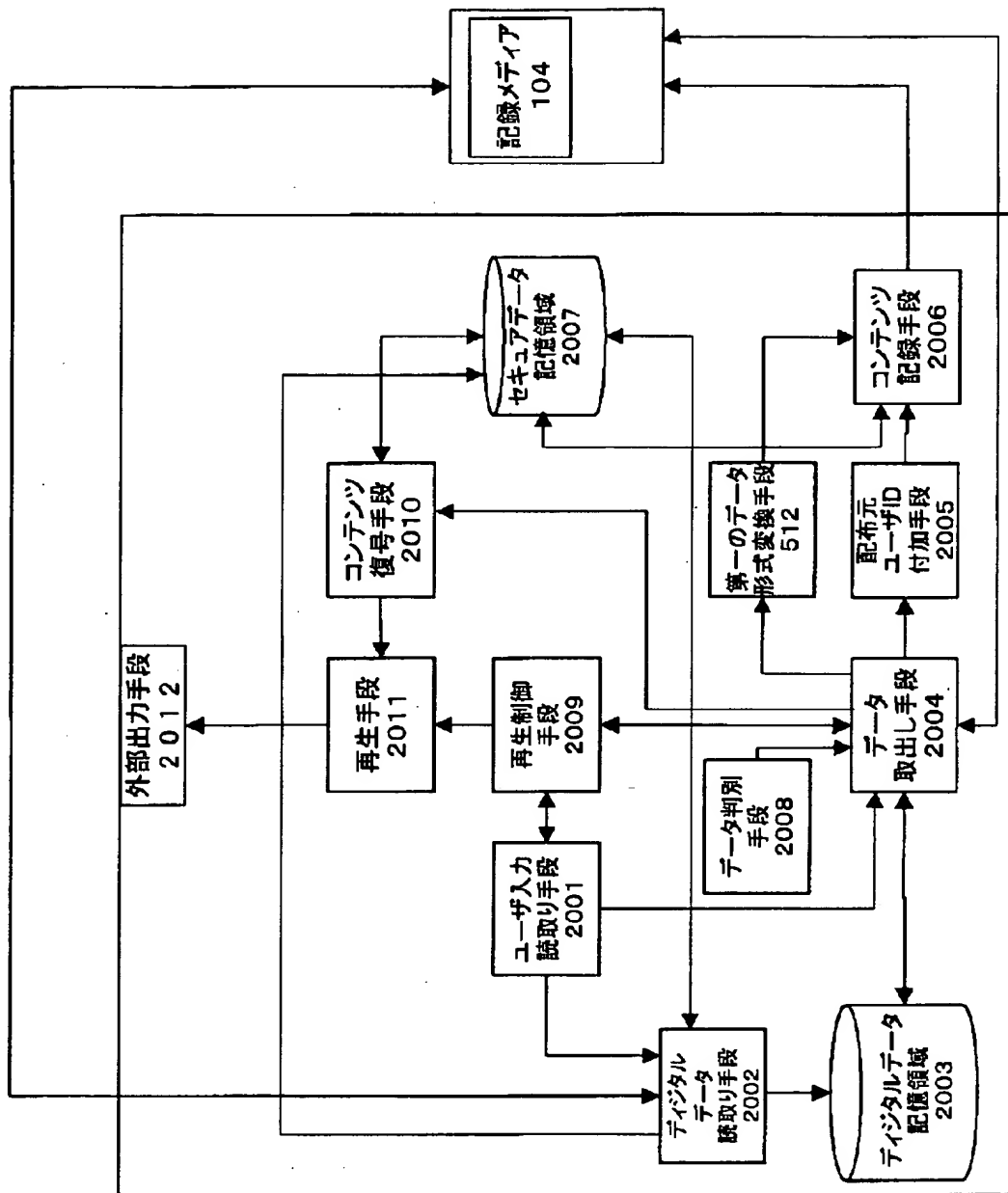


【図 1 9】



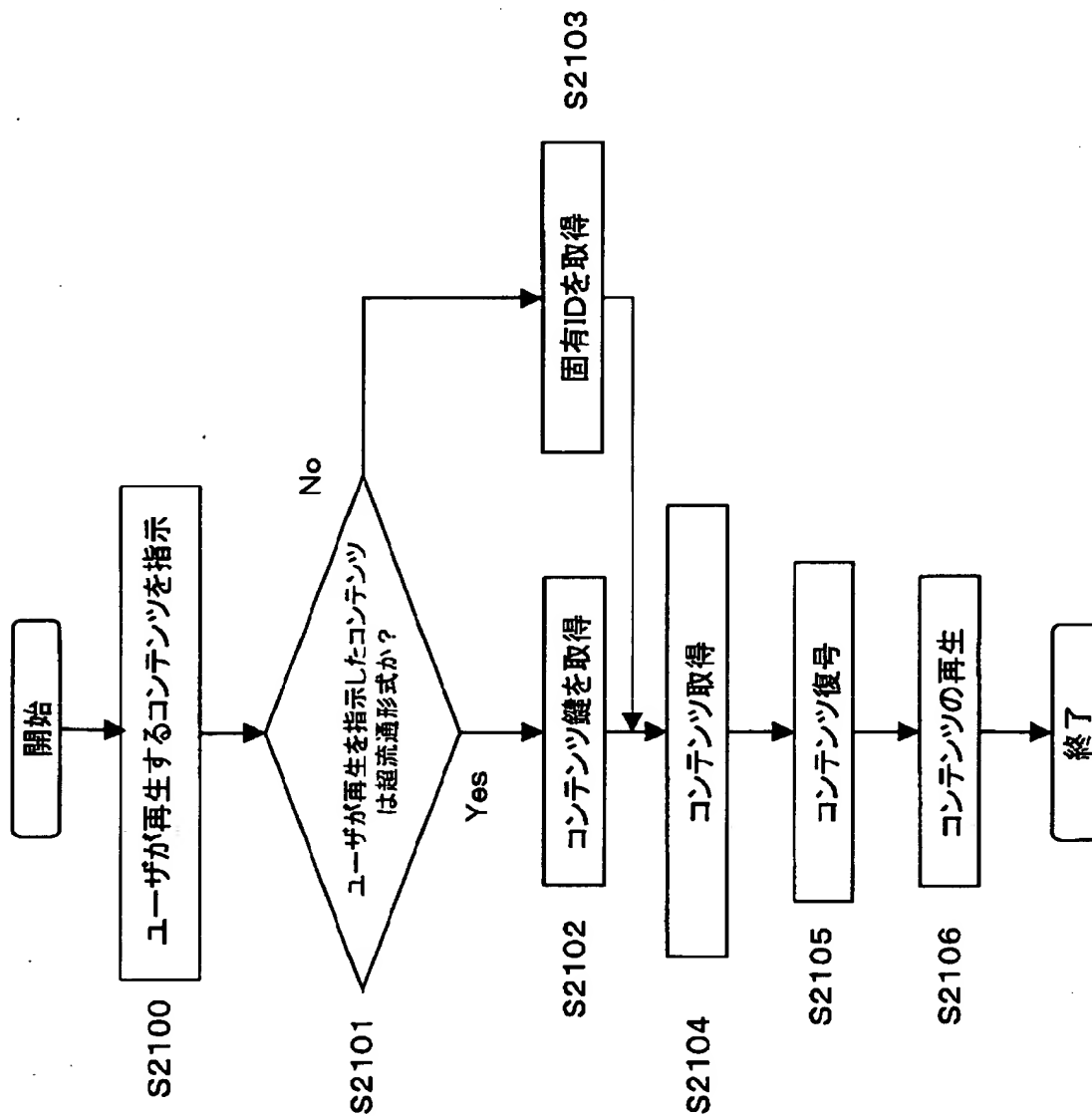
サーバ1801

【図 2 0】



デジタルデータ記録再生装置 2 0 0 0

【図 2 1】



【書類名】 要約書

【要約】

【課題】 半導体メモリにデジタルデータを記録するとき、記録メディアを用いたデジタルデータの二次配布が可能な形で記録することができる情報処理装置を提供することを目的とする。

【解決手段】 本発明における情報処理装置であるデジタルデータ記録再生装置 1 0 1 (a) は、ユーザ入力読取り手段 5 0 0、超流通形式データ受信手段 5 0 1、超流通形式データ記憶領域 5 0 2、データ取出し手段 5 0 3、配布元ユーザ I D 付加手段 5 0 4、コンテンツ記録手段 5 0 5、購入処理手段 5 0 6、セキュアデータ記憶領域 5 0 7、コンテンツ復号手段 5 0 8、再生制御手段 5 0 9、再生手段 5 1 0、外部出力手段 5 1 1 から構成される。

【選択図】 図 5

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社